Advanced Threat Prevention Administration

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.

- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.

- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

May 18, 2023

Table of Contents

4

Advanced Threat Prevention

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

The Palo Alto Networks® next-generation firewall threat intrusion prevention subscriptions protect and defend your network from commodity threats and advanced persistent threats (APTs) using multi-pronged detection mechanisms to combat the entire gamut of the threat landscape. Palo Alto Networks threat prevention solution is comprised of the following subscriptions:

- **Advanced Threat Prevention**—The Advanced Threat Prevention cloud service uses inline deep learning and machine learning models for real-time detection of evasive and never before seen, unknown C2 threats and zero day vulnerability exploits. As an ultra low-latency native cloud service, this extensible and infinitely scalable solution is always kept up to date with model training improvements. It also supports Local Deep Learning, which complements the cloud-based Inline Cloud Analysis component of Advanced Threat Prevention by providing a mechanism to perform fast, local deep learning-based analysis of zero-day and other evasive threats. The Advanced Threat Prevention license includes all of the benefits included with Threat Prevention.

- **Threat Prevention**—The base Threat Prevention subscription is based on signatures generated from malicious traffic data collected from various Palo Alto Networks services. These signatures are used by the firewall to enforce security policies based on specific threats, which include: command-and-control (C2), various types of known malware, and vulnerability exploits; and combined with App-ID and User-ID identification technologies on the firewall, you can cross-reference context data to produce fine grained policies. As a part of your threat mitigation policies, you can also identify and block known or risky file types and IP addresses, of which several premade categories are available, including lists specifying bulletproof service providers and known malicious IPs. In cases where specialized tools and software are used, you can create your own vulnerability signatures to customize your intrusion prevention capabilities to your network's unique requirements.

To maximize your threat prevention, Palo Alto Network also recommends the following subscription services in addition to Advanced | Threat Prevention:

- **DNS Security**—The DNS Security cloud service designed to protect your organization from advanced DNS-based threats. By applying advanced machine learning and predictive analytics to a diverse range of threat intelligence sources, DNS Security generates an enhanced DNS signature set and provides real-time analysis of DNS requests to defend your network against newly generated malicious domains. DNS Security can detect various C2 threats, including

DNS tunneling, DNS rebinding attacks, domains created using auto-generation, malware hosts, and many more. DNS Security requires and works with your Advanced Threat Prevention or Threat Prevention subscription for complete DNS threat coverage.

Palo Alto Networks intrusion prevention subscriptions work together to provide a comprehensive solution that intercepts and breaks the chain at various stages of the attack process and provides visibility to prevent security infringement on your network infrastructure.

Advanced Threat Prevention Detection Services

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Advanced Threat Prevention is an intrusion prevention system (IPS) solution that can detect and block malware, vulnerability exploits, and command-and-control (C2) across all ports and protocols, using a multi-layered prevention system with components operating on the firewall and in the cloud. The Threat Prevention cloud operates a multitude of detection services using the combined threat data from Palo Alto Networks services to create signatures, each possessing specific identifiable patterns, and are used by the firewall to enforce security policies when matching threats and malicious behaviors are detected. These signatures are categorized based on the threat type and are assigned unique identifier numbers. To detect threats that correspond with these signatures, the firewall operates analysis engines that inspect and classify network traffic exhibiting anomalous traits.

In addition to the signature-based detection mechanism, Advanced Threat Prevention provides an inline detection system to prevent unknown and evasive C2 threats, including those produced through the Empire framework, as well as command injection and SQL injection vulnerabilities. The Advanced Threat Prevention cloud operates extensible deep learning models that enable inline analysis capabilities on the firewall, on a per-request basis to prevent zero-day threats from entering the network as well as to distribute protections. This allows you to prevent unknown threats using real-time traffic inspection with inline detectors. These deep learning, ML-based detection engines in the Advanced Threat Prevention cloud analyze traffic for unknown C2 and vulnerabilities which utilize SQL injection and command injection to protect against zero-day threats. To provide a threat context and comprehensive detection details, reports are generated that can include the tools/techniques used by the attacker, the scope and impact of the detection, as well as the corresponding cyberattack classification as defined by the MITRE ATT&CK® framework.

> *MITRE ATT&CK® is a curated knowledge base and model for cyber adversary behavior. This work is reproduced and distributed with the permission of The MITRE Corporation. The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.*

By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download

content packages or operate process intensive, firewall-based analyzers which consume resources. The cloud-based detection engine logic is continuously monitored and updated using C2 traffic datasets from WildFire, with additional support from Palo Alto Networks threat researchers who provide human intervention for highly accurized detection enhancements. Advanced Threat Prevention's deep learning engines support analysis of C2-based threats over HTTP, HTTP2, SSL, unknown-UDP, and unknown-TCP applications. Additional analysis models are delivered through content updates, however, enhancements to existing models are performed as a cloud-side update, requiring no firewall update.

Advanced Threat Prevention also supports Local Deep Learning, which provides a mechanism to perform fast, local deep learning-based analysis of zero-day and other evasive threats, as a complementary feature to the cloud-based Inline Cloud Analysis component of Advanced Threat Prevention. Known malicious traffic that matches against Palo Alto Networks published signature set are dropped (or have another user-defined action applied to them); however, certain traffic that matches the criteria for suspicious content are rerouted for analysis using the Deep Leaning Analysis detection module. If further analysis is necessary, the traffic is sent to the Advanced Threat Prevention cloud for additional analysis, as well as the requisite false-positive and false-negative checks. The Deep Learning detection module is based on the proven detection modules operating in the Advanced Threat Prevention cloud, and as such, have the same zero-day and advanced threat detection capabilities. However, they also have the added advantage of processing a much higher volume of traffic, without the lag associated with cloud queries. This enables you to inspect more traffic and receive verdicts in a shorter span of time. This is especially beneficial when faced with challenging network conditions.

📋 *Palo Alto Networks also offers the Threat Prevention subscription that does not include the features found in the cloud-based Advanced Threat Prevention license.*

The threat signatures used by the firewall are broadly categorized into three types: antivirus, anti-spyware, vulnerability and are used by the corresponding security profiles to enforce user-defined policies.

📋 *Palo Alto Networks cloud-delivered security services also generate WildFire and DNS C2 signatures for their respective services, as well as file-format signatures, which can designate file types in lieu of threat signatures; for example, as signature exceptions.*

- Antivirus signatures detect various types of malware and viruses, including worms, trojans, and spyware downloads.

- Anti-Spyware signatures detect C2 spyware on compromised hosts from trying to phone-home or beacon out to an external C2 server.

- Vulnerability signatures detect exploit system vulnerabilities.

Signatures have a default severity level with an associated default action; for example, in the case of a highly malicious threat, the default action is Reset Both. This setting is based on security recommendations from Palo Alto Networks.

In deployments where specialized internal applications are present or in cases where third-party intelligence feeds using open-source Snort and Suricata rules, custom signatures can be created for purpose-built protection.

Firewalls receive signature updates in the form of two update packages: the daily Antivirus Content and weekly Application and Threats Content updates. The antivirus content updates include antivirus signatures and DNS (C2) signatures used by antivirus and anti-spyware security profiles, respectively. Content updates for applications and threats include vulnerability and anti-spyware signatures, used by the vulnerability and anti-spyware security profiles, respectively. The update packages also include additional content leveraged by other services and sub-functions. For more information, refer to Dynamic Content Updates.

Threat Signature Categories

Where Can I Use This?	What Do I Need?
- Prisma Access (Managed by Strata Cloud Manager) - Prisma Access (Managed by Panorama) - NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

There are three types of Palo Alto Networks threat signatures, each designed to detect different types of threats as the network traffic is scanned:

- Antivirus signatures—Detect viruses and malware found in executables and file types.
- Anti-spyware signatures—Detects command-and-control (C2) activity, where spyware on an infected client is collecting data without the user's consent and/or communicating with a remote attacker.
- Vulnerability signatures—Detects system flaws that an attacker might otherwise attempt to exploit.

A signature's severity indicates the risk of the detected event, and a signature's default action (for example, block or alert) is how Palo Alto Networks recommends that you enforce matching traffic.

You must Set Up Antivirus, Anti-Spyware, and Vulnerability Protection to define what action to take when a threat is detected, and you can easily use the default security profiles to start blocking threats based on Palo Alto Networks recommendations. For each signature type, category, and even specific signatures you can continue to modify or create new profiles to more granularly enforce potential threats.

The following table lists all possible signature categories by type—Antivirus, Spyware, and Vulnerability—and includes the content update (Applications and Threats, Antivirus, or WildFire) that provides the signatures in each category. You can also go to the Palo Alto Networks Threat Vault to Learn More About Threat Signatures.

Threat Category	Content Update that Provides These Signatures	Description
Antivirus Signatures		
apk	Antivirus WildFire	Malicious Android Application (APK) files.

Threat Category	Content Update that Provides These Signatures	Description
MacOSX	Antivirus WildFire	Malicious MacOSX files, including: • Apple disk image (DMG) files. • Mach object files (Mach-O) are executables, libraries, and object code. • Apple software installer packages (PKGs)
flash	Antivirus Wildfire or WildFire Private	Adobe Flash applets and Flash content embedded in web pages.
jar	Antivirus Wildfire	Java applets (JAR/class file types).
ms-office	Antivirus Wildfire or WildFire Private	Microsoft Office files, including documents (DOC, DOCX, RTF), workbooks (XLS, XLSX), and PowerPoint presentations (PPT, PPTX). This also includes Office Open XML (OOXML) 2007+ documents.
pdf	Antivirus Wildfire or WildFire Private	Portable Document Format (PDF) files.
pe	Antivirus Wildfire or WildFire Private	Portable executable (PE) files can automatically execute on a Microsoft Windows system and should be only allowed when authorized. These files types include: • Object code. • Fonts (FONs). • System files (SYS). • Driver files (DRV). • Windows control panel items (CPLs). • DLLs (dynamic-link libraries). • OCXs (libraries for OLE custom controls, or ActiveX controls). • Windows screensaver files (SCRs). • Extensible Firmware Interface (EFI) files, which run between an OS and firmware in order to facilitate device updates and boot operations. • Program information files (PIFs).

Threat Category	Content Update that Provides These Signatures	Description
linux	Antivirus Wildfire	Executable and Linkable Format (ELF) files.
archive	Antivirus Wildfire	Roshal Archive (RAR) and 7-Zip (7z) archive files.

Spyware Signatures

adware	Applications and Threats	Detects programs that display potentially unwanted advertisements. Some adware modifies browsers to highlight and hyperlink the most frequently searched keywords on web pages-these links redirect users to advertising websites. Adware can also retrieve updates from a command-and-control (C2) server and install those updates in a browser or onto a client system. Newly-released protections in this category are rare.
autogen	Antivirus	These payload-based signatures detect command-and-control (C2) traffic and are automatically-generated. Importantly, autogen signatures can detect C2 traffic even when the C2 host is unknown or changes rapidly.
backdoor	Applications and Threats	Detects a program that allows an attacker to gain unauthorized remote access to a system.
botnet	Applications and Threats	Indicates botnet activity. A botnet is a network of malware-infected computers ("bots") that an attacker controls. The attacker can centrally command every computer in a botnet to simultaneously carry out a coordinated action (like launching a DoS attack, for example).
browser-hijack	Applications and Threats	Detects a plugin or software that is modifying browser settings. A browser hijacker might take over auto search or track users' web activity and send this information to a C2 server. Newly-released protections in this category are rare.
cryptominer	Applications and Threats	(Sometimes known as cryptojacking or miners) Detects the download attempt or network traffic generated from malicious programs designed to use computing resources to mine cryptocurrencies without the user's knowledge. Cryptominer binaries are frequently

Threat Category	Content Update that Provides These Signatures	Description
		delivered by a shell script downloader that attempts to determine system architecture and kill other miner processes on the system. Some miners execute within other processes, such as a web browser rendering a malicious web page.
data-theft	Applications and Threats	Detects a system sending information to a known C2 server. Newly-released protections in this category are rare.
dns	Antivirus	Detects DNS requests to connect to malicious domains. dns and dns-wildfire signatures detect the same malicious domains; however, dns signatures are included in the daily Antivirus content update and dns-wildfire signatures are included in the WildFire updates that release protections every 5 minutes.
dns-security	Antivirus	Detects DNS requests to connect to malicious domains. dns-security includes signatures from dns and dns-wildfire in addition to the unique signatures generated by the DNS Security service.
dns-wildfire	Wildfire or WildFire Private	Detects DNS requests to connect to malicious domains. dns and dns-wildfire signatures detect the same malicious domains; however, dns signatures are included in the daily Antivirus content update and dns-wildfire signatures are included in the WildFire updates that release protections every 5 minutes.
downloader	Applications and Threats	(Also known as droppers, stagers, or loaders) Detects programs that use an internet connection to connect to a remote server to download and execute malware on the compromised system. The most common use case is for a downloader to be deployed as the culmination of *stage one* of a cyber attack, where the downloader's fetched payload execution is considered *second stage*. Shell scripts (Bash, PowerShell, etc.), trojans, and malicious lure documents (also known as maldocs) such as PDFs and Word files are common downloader types.
fraud	Applications and Threats	(Including form-jacking, phishing, and scams) Detects access to compromised websites that have been determined to be injected with malicious JavaScript code to collect sensitive user information. (for example,

Threat Category	Content Update that Provides These Signatures	Description
		Name, address, email, credit card number, CVV, expiration date) from payment forms that are captured on the checkout pages of e-commerce websites.
hacktool	Applications and Threats	Detects traffic generated by software tools that are used by malicious actors to conduct reconnaissance, attack or gain access to vulnerable systems, exfiltrate data, or create a command and control channel to surreptitiously control a computer system without authorization. These programs are strongly associated with malware and cyber attacks. Hacking tools might be deployed in a benign manner when used in Red and Blue Team operations, penetration tests, and R&D. The use or possession of these tools may be illegal in some countries, regardless of intent.
keylogger	Applications and Threats	Detects programs that allow attackers to secretly track user activity, by logging keystrokes and capturing screenshots. Keyloggers use various C2 methods to periodically sends logs and reports to a predefined e-mail address or a C2 server. Through keylogger surveillance, an attacker could retrieve credentials that would enable network access.
networm	Applications and Threats	Detects a program that self-replicates and spreads from system to system. Net-worms might use shared resources or leverage security failures to access target systems.
phishing-kit	Applications and Threats	Detects when a user attempts to connect to a phishing kit landing page (likely after receiving an email with a link to the malicious site). A phishing website tricks users into submitting credentials that an attacker can steal to gain access to the network. *In addition to blocking access to phishing kit landing pages, enable* Multi-Factor Authentication *and* Prevent Credential Phishing *to prevent phishing attacks at all stages.*
post-exploitation	Applications and Threats	Detects activity that indicates the post-exploitation phase of an attack, where an attacker attempts to assess the value of a compromised system. This might

Threat Category	Content Update that Provides These Signatures	Description
		include evaluating the sensitivity of the data stored on the system, and the system's usefulness in further compromising the network.
webshell	Applications and Threats	Detects web shells and web shell traffic, including implant detection and command and control interaction. Web shells must first be implanted by a malicious actor onto the compromised host, most often targeting a web server or framework. Subsequent communication with the web shell file frequently enables a malicious actor to establish a foothold in the system, conduct service and network enumeration, data exfiltration, and remote code execution in the context of the web server user. The most common web shell types are PHP, .NET, and Perl markup scripts. Attackers can also use web shell-infected web servers (the web servers can be both internet-facing or internal systems) to target other internal systems.
spyware	Applications and Threats	Detect outbound C2 communication. These signatures are either auto-generated or are manually created by Palo Alto Networks researchers. *Spyware and autogen signatures both detect outbound C2 communication; however, autogen signatures are payload-based and can uniquely detect C2 communications with C2 hosts that are unknown or change rapidly.*

Vulnerability Signatures

brute force	Applications and Threats	A brute-force signature detects multiple occurrences of a condition in a particular time frame. While the activity in isolation might be benign, the brute-force signature indicates that the frequency and rate at which the activity occurred is suspect. For example, a single FTP login failure does not indicate malicious activity. However, many failed FTP logins in a short period likely indicate an attacker attempting password combinations to access an FTP server. You can tune the action and trigger conditions for brute force signatures.

Threat Category	Content Update that Provides These Signatures	Description
code execution	Applications and Threats	Detects a code execution vulnerability that an attacker can leverage to run code on a system with the privileges of the logged-in user.
code-obfuscation	Applications and Threats	Detects code that has been transformed to conceal certain data while retaining its function. Obfuscated code is difficult or impossible to read, so it's not apparent what commands the code is executing or with which programs its designed to interact. Most commonly, malicious actors obfuscate code to conceal malware. More rarely, legitimate developers might obfuscate code to protect privacy, intellectual property, or to improve user experience. For example, certain types of obfuscation (like minification) reduce file size, which decreases website load times and bandwidth usage.
dos	Applications and Threats	Detects a denial-of-service (DoS) attack, where an attacker attempts to render a targeted system unavailable, temporarily disrupting the system and dependent applications and services. To perform a DoS attack, an attacker might flood a targeted system with traffic or send information that causes it to fail. DoS attacks deprive legitimate users (like employees, members, and account holders) of the service or resource to which they expect access.
exploit-kit	Applications and Threats	Detects an exploit kit landing page. Exploit kit landing pages often contain several exploits that target one or many common vulnerabilities and exposures (CVEs), for multiple browsers and plugins. Because the targeted CVEs change quickly, exploit-kit signatures trigger based on the exploit kit landing page, and not the CVEs. When a user visits a website with an exploit kit, the exploit kit scans for the targeted CVEs and attempts to silently deliver a malicious payload to the victim's computer.
info-leak	Applications and Threats	Detects a software vulnerability that an attacker could exploit to steal sensitive or proprietary information. Often, an info-leak might exist because comprehensive checks do not exist to guard the data, and attackers can exploit info-leaks by sending crafted requests.

Threat Category	Content Update that Provides These Signatures	Description
insecure-credentials	Applications and Threats	Detects the use of weak, compromised, and manufacturer default passwords for software, network appliances, and IoT devices.
overflow	Applications and Threats	Detects an overflow vulnerability, where a lack of proper checks on requests could be exploited by an attacker. A successful attack could lead to remote code execution with the privileges of the application, server or operating system.
phishing	Applications and Threats	Detects when a user attempts to connect to a phishing kit landing page (likely after receiving an email with a link to the malicious site). A phishing website tricks users into submitting credentials that an attacker can steal to gain access to the network. 💡 *In addition to blocking access to phishing kit landing pages, enable* Multi-Factor Authentication *and* Prevent Credential Phishing *to prevent phishing attacks at all stages.*
protocol-anomaly	Applications and Threats	Detects protocol anomalies, where a protocol behavior deviates from standard and compliant usage. For example, a malformed packet, poorly-written application, or an application running on a non-standard port would all be considered protocol anomalies, and could be used as evasion tools. It is a best practice to block protocol anomalies of any severity.
sql-injection	Applications and Threats	Detects a common hacking technique where an attacker inserts SQL queries into an application's requests, in order to read from or modify a database. This type of technique is often used on websites that do not comprehensively sanitize user input.

Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

To monitor and protect your network from most Layer 4 and Layer 7 attacks, here are a few recommendations.

❑ Upgrade to the most current PAN-OS software version and content release version to ensure that you have the latest security updates. See Install Content and Software Updates.

❑ Enable DNS Security (requires a Threat Prevention and DNS Security subscription license) to sinkhole malicious DNS requests. Palo Alto Networks recommends using the following DNS Security category configuration settings in your Anti-Spyware profile:

☐ SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
⌄ : Palo Alto Networks Content			
☐ default-paloalto-dns		sinkhole	extended-capture
⌄ : DNS Security			
☐ Command and Control Domains	default (high)	sinkhole	extended-capture
☐ Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
☐ Grayware Domains	default (low)	sinkhole	disable
☐ Malware Domains	default (medium)	sinkhole	disable
☐ Parked Domains	default (informational)	sinkhole	disable
☐ Phishing Domains	default (low)	sinkhole	disable
☐ Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
☐ Newly Registered Domains	default (informational)	sinkhole	disable

• For the log severity settings, use the default settings:

• For the policy action, set all signature sources to **sinkhole**.

• For packet capture, set Command and Control Domains to **extended-capture**. Leave all other categories to default settings.

For more information on related anti-spyware settings, see Best Practice Internet Gateway Anti-Spyware Profile.

❑ If you have an active Advanced Threat Prevention subscription, enable Inline Cloud Analysis and Local Deep Learning, where available, to block advanced C2 and spyware threats in real-time. The default action for each analysis engine is **alert**, which generates a threat log when a corresponding threat is detected; however, Palo Alto Networks recommends setting all analysis model actions to **Reset-Both**. This drops matching packets and sends an RST to the client and server, breaking the connection, as well as generating a threat log entry.

❑ Set up the firewall to act as a DNS proxy and enable evasion signatures:

🗒️ *DNS proxy is not part of the firewall security policy engine; instead, it directs the firewall to resolve DNS hostnames, while maintaining domain to IP mapping, which is crucial for preventing TLS/HTTP evasion.*

- Configure a DNS Proxy Object.

  When acting as a DNS proxy, the firewall resolves DNS requests and caches hostname-to-IP address mappings to quickly and efficiently resolve future DNS queries.

- Enable Evasion Signatures

  Evasion signatures that detect crafted HTTP or TLS requests can send alerts when clients connect to a domain other than the domain specified in the original DNS request. Make sure to configure DNS proxy before you enable evasion signatures. Without DNS proxy, evasion signatures can trigger alerts when a DNS server in the DNS load balancing configuration returns different IP addresses—for servers hosting identical resources—to the firewall and client in response to the same DNS request.

Anti-Spyware Profile ⓘ ▭

Name	Evasion Protection
Description	

Signature Policies | **Signature Exceptions** | DNS Policies | DNS Exceptions

🔍 evasion   2 / 10344 → ✕

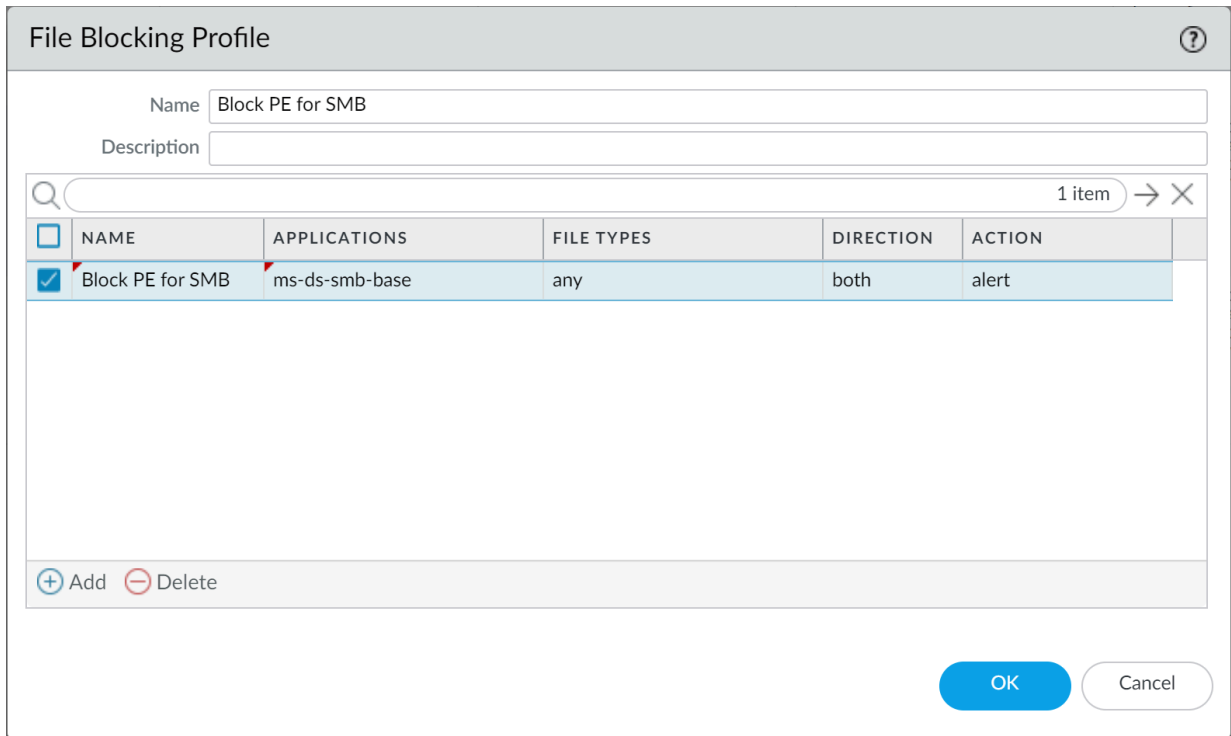| ENAB…	ID	THREAT NAME	IP ADDRESS EXEMPTIONS	POLICY	CATEGORY	SEVERITY	ACTION	PACKET CAPTURE	
☑	149…	Suspicious TLS Evasion Found			spyware	informational	default (allow)	disable	
☑	149…	Suspicious HTTP Evasion Found			spyware	informational	default (allow)	disable	

☑ Show all signatures 🄿 PDF/CSV   ⏮ ◀ | Page 1 of 1 | ▶ ⏭ | ↻ Displaying 1 - 2/ 2 threats

OK   Cancel

❑ For deployments operating Prisma Access or networks without an internal DNS server, configure your DNS policy to use the Palo Alto Networks sinkhole IP address (72.5.65.111) instead of the default sinkhole FQDN (sinkhole.paloaltonetworks.com).

The DNS sinkhole used by the Anti-Spyware Profile enables the firewall to forge a response to a DNS query for domains that match the category configured for a sinkhole action to the specified sinkhole server, to assist in identifying compromised hosts. When the default sinkhole FQDN is used, the firewall sends the CNAME record as a response to the client, with the expectation that an internal DNS server will resolve the CNAME record, allowing malicious communications from the client to the configured sinkhole server to be logged and readily identifiable. However, if clients are operating Prisma Access, are in networks without an internal DNS server, or using other software or tools that cannot be properly resolve a CNAME into an A record response, the DNS request is dropped, resulting in incomplete traffic log details that are crucial for threat analysis.

❑ For servers, create Security policy rules to allow only the application(s) that you sanction on each server. Verify that the standard port for the application matches the listening port on the server. For example, to ensure that only SMTP traffic is allowed to your email server, set the Application to **smtp** and set the Service to **application-default**. If your server uses only a subset of the standard ports (for example, if your SMTP server uses only port 587 while the SMTP application has standard ports defined as 25 and 587), create a new custom service that includes only port 587 and use that new service in your security policy rule instead of application-default. Additionally, make sure you restrict access to specific source and destinations zones and sets of IP addresses.

❑ Block all unknown applications and traffic using the Security policy. Typically, the only applications classified as unknown traffic are internal or custom applications on your network and potential threats. Unknown traffic can be either non-compliant applications or protocols that are anomalous or abnormal or it can be known applications that are using non-standard ports, both of which should be blocked. See Manage Custom or Unknown Applications.

❑ Set Up File Blocking to block Portable Executable (PE) file types for internet-based SMB (Server Message Block) traffic from traversing trust to untrust zones (ms-ds-smb applications).

	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
☑	Block PE for SMB	ms-ds-smb-base	any	both	alert

File Blocking Profile

Name: Block PE for SMB

Description:

1 item

⊕ Add ⊖ Delete

OK   Cancel

❑ Block malicious variants of PE (portable executables), ELF and MS Office files, and PowerShell and shell scripts in real-time. Enabling WildFire Inline ML allows you to dynamically analyze files using machine learning on the firewall. This additional layer of antivirus protection complements the WildFire-based signatures to provide extended coverage for files of which signatures do not already exist.

❑ Create a Zone Protection profile that is configured to protect against packet-based attacks (**Network** > **Network Profiles** > **Zone Protection**):

- Select the option to drop **Malformed** IP packets (**Packet Based Attack Protection** > **IP Drop**).

- Enable the drop **Mismatched overlapping TCP segment** option (**Packet Based Attack Protection** > **TCP Drop**).

  By deliberately constructing connections with overlapping but different data in them, attackers attempt to cause misinterpretation of the intent of the connection and deliberately induce false positives or false negatives. Attackers also use IP spoofing and sequence number prediction to intercept a user's connection and inject their own data into that connection. Selecting the **Mismatched overlapping TCP segment** option specifies that PAN-OS discards frames with mismatched and overlapping data. Received segments are

discarded when they are contained within another segment, when they overlap with part of another segment, or when they contain another complete segment.

- Enable the drop **TCP SYN with Data** and drop **TCP SYNACK with Data** options (**Packet Based Attack Protection** > **TCP Drop**).

  Dropping SYN and SYN-ACK packets that contain data in the payload during a three-way handshake increases security by blocking malware contained in the payload and preventing it from extracting unauthorized data before the TCP handshake is completed.

- Strip TCP timestamps from SYN packets before the firewall forwards the packet (**Packet Based Attack Protection** > **TCP Drop**).

  When you enable the **Strip TCP Options - TCP Timestamp** option, the TCP stack on both ends of the TCP connection will not support TCP timestamps. This prevents attacks that use different timestamps on multiple packets for the same sequence number.

Zone Protection Profile	?

Name: my-zone-protect

Description:

Flood Protection | Reconnaissance Protection | **Packet Based Attack Protection** | Protocol Protection | Ethernet SGT Protecti

IP Drop | **TCP Drop** | ICMP Drop | IPv6 Drop | ICMPv6 Drop

- ☑ Mismatched overlapping TCP segment
- ☐ Split Handshake
- ☑ TCP SYN with Data
- ☑ TCP SYNACK with Data

Reject Non-SYN TCP: global

Asymmetric Path: global

Strip TCP Options
- ☑ TCP Timestamp
- ☐ TCP Fast Open

Multipath TCP (MPTCP) Options: global

OK | Cancel

❑ If you configure IPv6 addresses on your network hosts, be sure to enable support for IPv6 if not already enabled (**Network** > **Interfaces** > **Ethernet > IPv6**).

Enabling support for IPv6 allows access to IPv6 hosts and also filters IPv6 packets encapsulated in IPv4 packets, which prevents IPv6 over IPv4 multicast addresses from being leveraged for network reconnaissance.

Ethernet Interface	
Interface Name	ethernet1/2
Comment	1.2.3.4/16
Interface Type	Layer3
Netflow Profile	SevOne

Config | IPv4 | **IPv6** | SD-WAN | Advanced

☑ Enable IPv6 on the interface

❑ Enable support for multicast traffic so that the firewall can enforce policy on multicast traffic (**Network** > **Virtual Router** > **Multicast**).

Virtual Router

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

☑ Enable

Rendezvous Point | Interfaces | SPT Threshold | Source Specific Address Space | Advanced

Local Rendezvous Point

RP Type | None

Remote Rendezvous Point

	IP ADDRESS	GROUP	OVERRIDE

⊕ Add ⊖ Delete

OK | Cancel

☐ Disable the options to **Forward datagrams exceeding UDP content inspection queue** and **Forward segments exceeding TCP content inspection queue** (**Device** > **Setup** > **Content-ID** > **Content-ID Settings**).
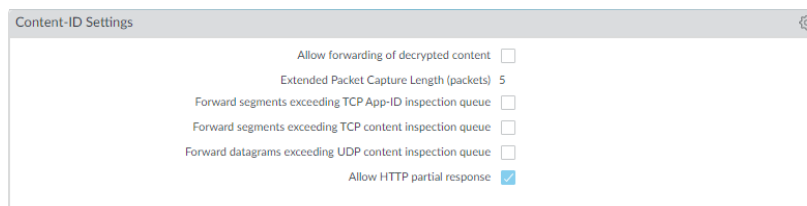
By default, when the TCP or UDP content inspection queues are full, the firewall skips content inspection for TCP segments or UDP datagrams that exceed the queue limit of 64. Disabling this option ensures content inspection for all TCP and UDP datagrams that the firewall allows. Only under specific circumstances—for example, if the firewall platform is not sized appropriately to align with a use case—could disabling this setting impact performance.

☐ Disable the **Allow HTTP partial response** (**Device** > **Setup** > **Content-ID** > **Content-ID Settings**).

The HTTP partial response option allows a client to fetch only part of a file. When a next-generation firewall in the path of a transfer identifies and drops a malicious file, it terminates the TCP session with an RST packet. If the web browser implements the HTTP header range option, it can start a new session to fetch only the remaining part of the file, which prevents the firewall from triggering the same signature again due to the lack of context into the initial session and, at the same time, allows the web browser to reassemble the file and deliver the malicious content. Disabling this option prevents this from happening.

Allow HTTP partial response is enabled on the firewall by default. This provides maximum availability but increases the risk of a successful cyberattack. For maximum security, disable this option to prevent the web browser from starting a new session to fetch the rest of a file after the firewall terminates the original session due to malicious activity. Disabling HTTP partial response affects HTTP-based data transfers which use the RANGE header, which may cause service anomalies for certain applications. After you disable HTTP partial response, validate the operation of your business-critical applications.

If you experience HTTP data transfer disruption on a business-critical application, you can create an Application Override policy for that specific application. Because Application Override bypasses App-ID (including threat and content inspection), create an Application Override policy for only the specific business-critical application, and specify sources and destinations to limit the rule (principle of least privilege access). Do not create Application Override policy unless you must. For information about Application Override policies, refer to https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0.

Content-ID Settings	
Allow forwarding of decrypted content	☐
Extended Packet Capture Length (packets)	5
Forward segments exceeding TCP App-ID inspection queue	☐
Forward segments exceeding TCP content inspection queue	☐
Forward datagrams exceeding UDP content inspection queue	☐
Allow HTTP partial response	☑

☐ Create a Vulnerability Protection Profile that blocks protocol anomalies and all vulnerabilities with low and higher severities.

A protocol anomaly occurs when a protocol behavior deviates from standard and compliant usage. For example, a malformed packet, poorly written application, or an application running on a non-standard port would all be considered protocol anomalies, and could be used as evasion tools.

If yours is a mission-critical network, where the business's highest priority is application availability, you should begin by alerting on protocol anomalies for a period of time to ensure

that no critical internal applications are using established protocols in a non-standard way. If you find that certain critical applications trigger protocol anomaly signatures, you can then exclude those applications from protocol anomaly enforcement. To do this, add another rule to the Vulnerability Protection Profile that allows protocol anomalies and attach the profile to the security policy rule that enforces traffic to and from the critical applications.

Make sure that Vulnerability Protection Profile rules and security policy rules that allow protocol anomalies for critical internal applications are listed above rules that block protocol anomalies. Traffic is evaluated against security policy rules and associated Vulnerability Protection Profiles rules from top to bottom, and is enforced based on the first matching rule.

- Begin by alerting on protocol anomalies:

  Create a Vulnerability Protection Profile rule with the **Action** set to Alert, the **Category** set to protocol-anomaly, and the **Severity** set to Any. Monitor your traffic to determine if any critical internal applications are using established protocols in non-standard ways. If you find

this to be true, continue to allow protocol anomalies for those applications, and then block protocol anomalies for all other applications.

Vulnerability Protection Rule

Rule Name	Alert on protocol anomalies

Threat Name	any

Used to match any signature containing the entered text as part of the signature name

Action	Alert	Packet Capture	extended-capture
Host Type	any	Category	protocol-anomaly

Any

☑ Any

☐ CVE ⌃

☑ Any

☐ VENDOR ID ⌃

Severity

☑ any (All severities)
☐ critical
☐ high
☐ medium
☐ low
☐ informational

⊕ Add   ⊖ Delete   ⊕ Add   ⊖ Delete

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

OK   Cancel

- Block protocol anomalies:

    Create a Vulnerability Protection Profile rule with the **Category** set to protocol-anomaly, the rule **Action** set to Reset Both, and the **Severity** set to Any.

- Optionally allow protocol anomalies for critical applications that use established protocols in a non-standard way. To do this, create a Vulnerability Protection Profile rule that allows protocol anomalies: set the rule **Action** to Allow, the **Category** to protocol-anomaly, and the

Severity to any. Attach the Vulnerability Protection Profile rule to the security policy rule that enforces traffic to and from critical applications.

- Add another rule to the Vulnerability Protection profile to block all vulnerabilities with low and higher severity. This rule must be listed after the rule that blocks protocol anomalies.

Vulnerability Protection Profile

Name	Best Practices Vulnerability
Description	

Rules | Exceptions

	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
✓	Block Protocol Anomalies	any	any	any		reset-both	disable
☐	Block all vulnerabilities	any	any	any	low medium high critical	reset-both	disable

⊕ Add   ⊖ Delete   ↑ Move Up   ↓ Move Down   ⊚ Clone   🔍 Find Matching Signatures

OK   Cancel

- ☐ Continue to attach the following security profiles to your Security policy rules to provide signature-based protection:

  - An Anti-Spyware profile to block all spyware with severity low and higher.

  - An Antivirus profile to block all content that matches an antivirus signature.

Share Threat Intelligence with Palo Alto Networks

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Telemetry is the process of collecting and transmitting data for analysis. When you enable telemetry on the firewall, the firewall periodically collects and sends information that includes applications, threats, and device health to Palo Alto Networks. Sharing threat intelligence provides the following benefits:

• Enhanced vulnerability and spyware signatures delivered to you and other customers worldwide. For example, when a threat event triggers vulnerability or spyware signatures, the firewall shares the URLs associated with the threat with the Palo Alto Networks threat research team, so they can properly classify the URLs as malicious.

• Rapid testing and evaluation of experimental threat signatures with no impact to your network, so that critical threat prevention signatures can be released to all Palo Alto Networks customers faster.

• Improved accuracy and malware detection abilities within PAN-DB URL filtering, DNS-based command-and-control (C2) signatures, and WildFire.

Palo Alto Networks uses the threat intelligence extracted from telemetry to deliver these benefits to you and other Palo Alto Networks users. All Palo Alto Networks users benefit from the telemetry data shared by each user, making telemetry a community-driven approach to threat prevention. Palo Alto Networks does not share your telemetry data with other customers or third-party organizations.

To read more about telemetry, including its benefits, usages, and configuration, see Device Telemetry.

Advanced Threat Prevention Resources

Where Can I Use This?	What Do I Need?
- Prisma Access (Managed by Strata Cloud Manager) - Prisma Access (Managed by Panorama) - NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

For more information on threat prevention best practices, refer to the following sources:

- Creating Custom Threat Signatures
- Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions
- URL Filtering Best Practices
- Zero Trust Best Practices
- DoS and Zone Protection Best Practices

To view a list of threats and applications that Palo Alto Networks products can identify, use the following links:

- Applipedia—Provides details on the applications that Palo Alto Networks can identify.
- Threat Vault—Lists threats that Palo Alto Networks products can identify. You can search by Vulnerability, Spyware, or Virus. Click the Details icon next to the ID number for more information about a threat.

32

Configure Threat Prevention

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Before you can enable and configure inline cloud analysis, you must obtain and install a Threat Prevention or Advanced Threat Prevention (to access the cloud-based inline cloud analysis features) in addition to any platform licenses from where it is operated. Licenses are activated from the Palo Alto Networks Customer Support Portal and must be active before you can enable any of the threat prevention features. Additionally, Threat Prevention (similar to other Palo Alto Networks security services) is administered through security profiles, which in turn is dependent on the configuration of network enforcement policies as defined through security policy rules. Before enabling Threat Prevention, it is recommended that you familiarize yourself core components of the security platform in which the security subscriptions are enabled. Refer to your product documentation for more information.

To enable and configure your Threat Prevention subscription to function optimally within your network security deployment, refer to the tasks below. While it may not be necessary to implement all of the processes shown here, Palo Alto Networks recommends reviewing all of the tasks to familiarize yourself with the available options for a successful deployment. It is additionally recommended that you follow the best practices provided by Palo Alto Networks for the optimum usability and security.

Set Up Antivirus, Anti-Spyware, and Vulnerability Protection

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Every Palo Alto Networks next-generation firewall comes with predefined Antivirus, Anti-Spyware, and Vulnerability Protection profiles that you can attach to Security policy rules. There is one predefined Antivirus profile, **default**, which uses the default action for each protocol (block HTTP, FTP, and SMB traffic and alert on SMTP, IMAP, and POP3 traffic). There are two predefined Anti-Spyware and Vulnerability Protection profiles:

- **default**—Applies the default action to all client and server critical, high, and medium severity spyware/vulnerability protection events. It does not detect low and informational events.
- **strict**—Applies the block response to all client and server critical, high and medium severity spyware/vulnerability protection events and uses the default action for low and informational events.

To ensure that the traffic entering your network is free from threats, attach the predefined profiles to your basic web access policies. As you monitor the traffic on your network and expand your policy rulebase, you can then design more granular profiles to address your specific security needs.

Use the following workflow to set up the default Antivirus, Anti-Spyware, and Vulnerability Protection Security Profiles.

- Strata Cloud Manager
- PAN-OS & Panorama

Set Up Antivirus, Anti-Spyware, and Vulnerability Protection (Cloud Management)

STEP 1 | Use the credentials associated with your Palo Alto Networks support account and log in to the Strata Cloud Manager on the hub.

The Threat Prevention subscription bundles the antivirus, anti-spyware, and vulnerability protection features in one license and is part of your Prisma Access subscription. For information about the applications and services offered with Prisma Access, refer to All

Available Apps and Services. To verify subscriptions for which you have currently-active licenses, Check What's Supported With Your License.

STEP 2 | (Optional) Create custom security profiles for antivirus, anti-spyware, and vulnerability protection.

Alternatively, you can use the predefined Best-Practice profiles.

> Transition safely *to* best practice Security profiles *for the best security posture.*

- To create custom WildFire and Antivirus Profiles, select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **WildFire and Antivirus** and **Add Profile**. Use the Antivirus profile transition steps to safely reach your goal.

- To create custom Anti-Spyware Profiles, select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Anti-Spyware** and **Add Profile**. Use the Anti-Spyware profile transition steps to safely reach your goal.

- To create custom Vulnerability Protection Profiles, select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Vulnerability Protection** and **Add Profile**. Use the Vulnerability Protection profile transition steps to safely reach your goal.

STEP 3 | Attach security profiles to your **Security Policy Rules**. Prisma Access enforces best practice security policy rules by default.

> 📋 *When you configure a Security policy rule that uses a Vulnerability Protection profile to block connections when exploits or attempts to gain unauthorized access are detected, Prisma Access automatically blocks that traffic and logs those incidents (see Monitor Blocked IP Addresses).*

1. Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Security Policy** and select the rule you want to modify or **Add Rule**.

2. In **Action and Advanced Inspection**, select the **Profile Group** and that includes the following security profiles: **WildFire and Antivirus**, **Anti-Spyware**, and **Vulnerability Protection**.

> 📋 *You can create new Profile groups in **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Profile Groups**. For more information, refer to Enable a Security Profile.*
>
> *By default, the **best-practice** profile group is enabled with the best-practice configuration for all available security profiles.*

Manage > Profile Group > Profile Group - Remote Networks

best-practice 🔒

Configuration   Usage

Profile Group

* Name	best-practice
Anti-Spyware Profile	best-practice ⌄
Vulnerability Protection Profile	best-practice ⌄
URL Access Management Profile	best-practice ⌄
File Blocking Profile	best-practice ⌄
HTTP Header Insertion Profile	None ⌄
WildFire and Antivirus Profile	best-practice ⌄
DNS Security Profile	best-practice ⌄

STEP 4 | Commit your changes.

Set Up Antivirus, Anti-Spyware, and Vulnerability Protection (NGFW (Managed by PAN-OS or Panorama))

> 💡 *Palo Alto Networks defines a default action for all anti-spyware and vulnerability protection signatures. To see the default action, select **Objects** > **Security Profiles** > **Anti-Spyware** or **Objects** > **Security Profiles** > **Vulnerability Protection** and then select a profile. Click the Exceptions tab and then click Show all signatures to view the list of the signatures and the corresponding default **Action**. To change the default action, create a new profile and specify an **Action**, and/or add individual signature exceptions to **Exceptions** in the profile.*

STEP 1 | Verify that you have a Threat Prevention subscription.

The Threat Prevention subscription bundles the antivirus, anti-spyware, and vulnerability protection features in one license. To verify that you have an active Threat Prevention subscription, select **Device** > **Licenses** and verify that the **Threat Prevention** expiration date is in the future.

Threat Prevention	
Date Issued	September 14, 2020
Date Expires	September 14, 2024
Description	Threat prevention subscription

STEP 2 | Download the latest content.

1. Select **Device** > **Dynamic Updates** and click **Check Now** at the bottom of the page to retrieve the latest signatures.

2. In the **Actions** column, click **Download** and install the latest Antivirus updates and then download and then **Install** the latest Applications and Threats updates.

STEP 3 | Schedule content updates.

Review the Best Practices for Applications and Threats Content Updates *for important information on deploying updates.*

1. Select **Device** > **Dynamic Updates** and then click **Schedule** to automatically retrieve signature updates for **Antivirus** and **Applications and Threats**.

2. Specify the frequency and timing for the updates:

   - **download-only**—The firewall automatically downloads the latest updates per the schedule you define but you must manually **Install** them.

   - **download-and-install**—The firewall automatically downloads and installs the updates per the schedule you define.

3. Click **OK** to save the update schedule; a commit is not required.

4. (Optional) Define a **Threshold** to indicate the minimum number of hours after an update becomes available before the firewall will download it. For example, setting the **Threshold** to **10** means the firewall will not download an update until it is at least 10 hours old regardless of the schedule.

5. (HA only) Decide whether to **Sync To Peer**, which enables peers to synchronize content updates after download and install (the update schedule does not sync across peers; you must manually configure the schedule on both peers).

   There are additional considerations for deciding if and how to **Sync To Peer** depending on your HA deployment:

   - **Active/Passive HA**—If the firewalls are using the MGT port for content updates, then schedule both firewalls to download and install updates independently. However, if the firewalls are using a data port for content updates, then the passive firewall will not download or install updates unless and until it becomes active. To keep the schedules in sync on both firewalls when using a data port for updates, schedule updates on both firewalls and then enable **Sync To Peer** so that whichever firewall is

active downloads and installs the updates and also pushes the updates to the passive firewall.

- **Active/Active HA**—If the firewalls are using the MGT interface for content updates, then select **download-and-install** on both firewalls but do not enable **Sync To Peer**. However, if the firewalls are using a data port, then select **download-and-install** on both firewalls and enable **Sync To Peer** so that if one firewall goes into the active-secondary state, the active-primary firewall will download and install the updates and push them to the active-secondary firewall.

STEP 4 | (Optional) Create custom security profiles for antivirus, anti-spyware, and vulnerability protection.

Alternatively, you can use the predefined default or strict profiles.

Transition safely *to* best practice Security profiles *for the best security posture.*

- To create custom Antivirus Profiles, select **Objects** > **Security Profiles** > **Antivirus** and **Add** a new profile. Use the Antivirus profile transition steps to safely reach your goal.
- To create custom Anti-Spyware Profiles, select **Objects** > **Security Profiles** > **Anti-Spyware** and **Add** a new profile. Use the Anti-Spyware profile transition steps to safely reach your goal.
- To create custom Vulnerability Protection Profiles, select **Objects** > **Security Profiles** > **Vulnerability Protection** and **Add** a new profile. Use the Vulnerability Protection profile transition steps to safely reach your goal.

STEP 5 | Attach security profiles to your Security policy rules.

> *When you configure the firewall with a Security policy rule that uses a Vulnerability Protection profile to block connections, the firewall automatically blocks that traffic in hardware (see* Monitor Blocked IP Addresses*).*

1. Select **Policies** > **Security** and select the rule you want to modify.
2. In the **Actions** tab, select **Profiles** as the **Profile Type**.
3. Select the security profiles you created for **Antivirus**, **Anti-Spyware**, and **Vulnerability Protection**.

Security Policy Rule	⑦

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action	Allow	⌄
	☐ Send ICMP Unreachable	

Profile Setting

Profile Type	Profiles	⌄
Antivirus	default	⌄
Vulnerability Protection	default	⌄
Anti-Spyware	default	⌄
URL Filtering	None	⌄
File Blocking	None	⌄
Data Filtering	None	⌄
WildFire Analysis	None	⌄

Log Setting

☐ Log at Session Start
☑ Log at Session End

Log Forwarding	Default	⌄

Other Settings

Schedule	None	⌄
QoS Marking	None	⌄
	☐ Disable Server Response Inspection	

OK   Cancel

STEP 6 | Commit your changes.

Click **Commit**.

Configure Inline Cloud Analysis

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support)

Inline Cloud Analysis is an Advanced Threat Prevention feature that enables the detection of advanced, highly-evasive zero-day command-and-control (C2) threats and command injection and SQL injection vulnerabilities in real-time by querying the Advanced Threat Prevention cloud service. Inline Cloud Analysis protection is delivered through your Anti-Spyware and Vulnerability Protection security profiles, with advanced C2 (command-and-control) and spyware threats handled by the former, and command injection and SQL injection vulnerabilities by the latter.

Supported firewalls operating PAN-OS 11.2 and later deployments can also access Local Deep Learning for Advanced Threat Prevention. Local Deep Learning complements the cloud-based Inline Cloud Analysis component of Advanced Threat Prevention by providing a mechanism to perform fast, local deep learning-based analysis of zero-day and other evasive threats. Updates to Local Deep Learning models are delivered through content updates. Due to the additional system resources necessary to run local Deep Learning detection modules, Local Deep Learning is only available on the following platforms:

• PA-5400 Series, excluding the PA-5450 appliance.

• VM-Series (must allocate at least 16GB of total memory)

• VM-Series Public Cloud

• VM-Series Private Cloud

To enable and configure Inline Cloud Analysis, and Local Deep Learning, you must activate your Advanced Threat Prevention license and create (or modify) the Anti-Spyware and Vulnerability Protection security profile. Then configure the policy settings for each category analysis engine and then attach the profiles to a security policy rule.

For more information on creating security policy rules, refer to the Policy chapter of the PAN-OS® Administrator's Guide.

• Strata Cloud Manager

• PAN-OS & Panorama

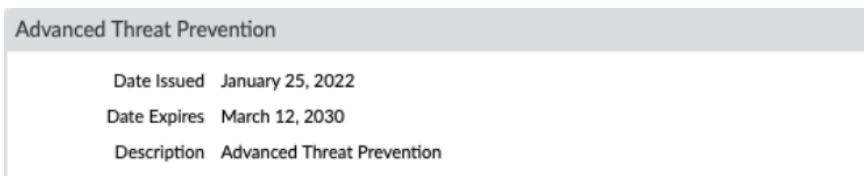# Configure Inline Cloud Analysis (PAN-OS & Panorama)

📋 *Advanced Threat Prevention Inline Cloud Analysis supports multiple detection engines, which require different minimum PAN-OS releases to enable:*

- *Detection of advanced C2 (command-and-control) and spyware threats requires PAN-OS 10.2 and later.*
- *Detection of zero-day exploit threats requires PAN-OS 11.0 and later.*
- *Support for LDL (Local Deep Learning) requires PAN-OS 11.2 and later.*

STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | To take advantage of inline cloud analysis, you must have an active Advanced Threat Prevention subscription.

To verify subscriptions for which you have currently-active licenses, select **Device** > **Licenses** and verify that the appropriate licenses are available and have not expired.

Advanced Threat Prevention	
Date Issued	January 25, 2022
Date Expires	March 12, 2030
Description	Advanced Threat Prevention

STEP 3 | Update or create a new Anti-Spyware Security profile to enable inline cloud analysis (to analyze traffic for advanced C2 (command-and-control) and spyware threats in real-time).
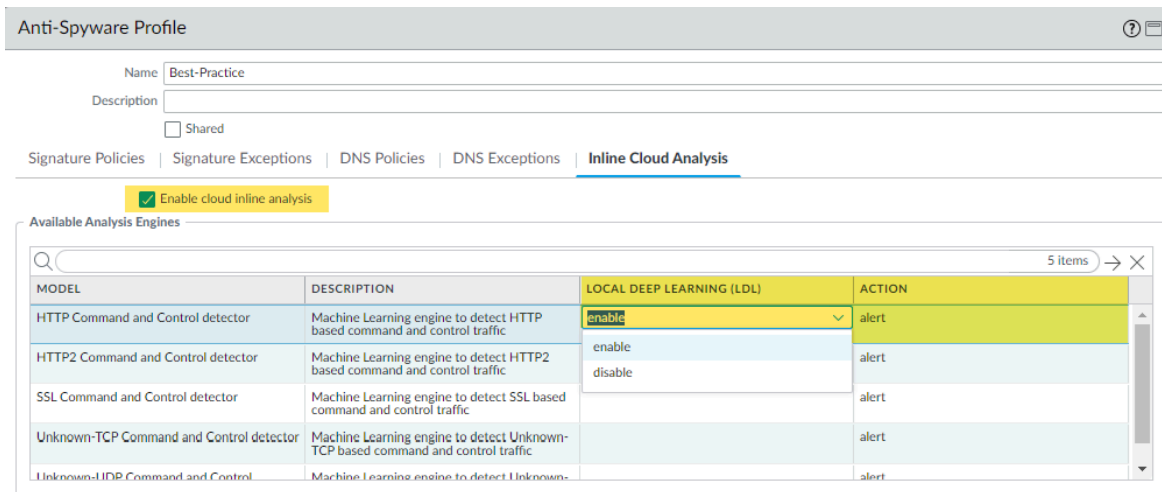
1. Select an existing **Anti-Spyware Profile** or **Add** a new one (**Objects** > **Security Profiles** > **Anti-Spyware**).
2. Select your Anti-Spyware profile and then go to **Inline Cloud Analysis** and **Enable inline cloud analysis**.
3. (Local Deep Learning [Supported in PAN-OS 11.2 and later]) Select **enable** for each available analysis engine with a **Local Deep Learning (LDL)** option. There are currently

two analysis engines available with an optional LDL mode: **HTTP Command and Control detector** and **HTTP2 Command and Control detector**.

4. Specify an **Action** to take when a threat is detected using a corresponding analysis engine.

> *The default action for each analysis engine is **alert**, however, Palo Alto Networks recommends setting all actions to **Reset-Both** for the best security posture.*

- **Allow**—The request is allowed and no log entry is generated.
- **Alert**—The request is allowed and a Threat log entry is generated.
- **Drop**—Drops the request; a reset action is not sent to the host/application.
- **Reset-Client**—Resets the client-side connection.
- **Reset-Server**—Resets the server-side connection.
- **Reset-Both**—Resets the connection on both the client and server ends.

5. Click **OK** to exit the Anti-Spyware Profile configuration dialog and **Commit** your changes.

STEP 4 | (Optional) Add URL and/or IP address exceptions to your Anti-Spyware profile if Inline Cloud Analysis produces false-positives. You can add exceptions by specifying an external dynamic list (URL or IP address list types) or an **Addresses** object.

1. Add an **External Dynamic Lists** or [IP] **Addresses** object exception.
2. Select **Objects > Security Profiles > Anti-Spyware**.
3. Select an Anti-Spyware profile for which you want to exclude specific URLs and/or IP addresses and then select **Inline Cloud Analysis**.
4. **Add** an **EDL URL** or **IP Address**, depending on the type of exception you want to add, and then select a pre-existing URL or IP address external dynamic list. If none are available, create a new external dynamic list. For IP address exceptions, you can, optionally, select an **Addresses** object list.

> *Anti-spyware profiles that are configured as **Shared** on Panorama-managed firewalls cannot have IP address objects added to the Inline Cloud Analysis exceptions list.*
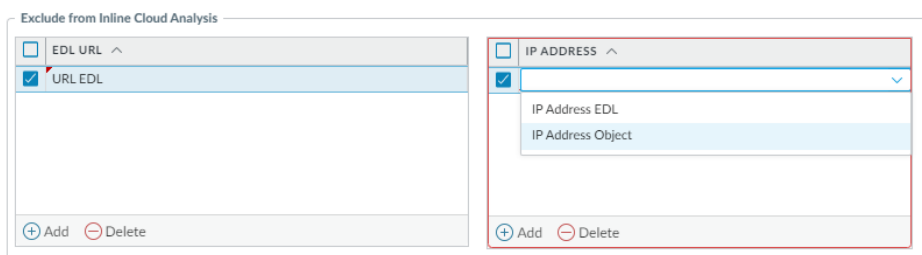
5. Click **OK** to save the Anti-Spyware profile and **Commit** your changes.

STEP 5 | (Supported in PAN-OS 11.0 and later) Update or create a new Vulnerability Protection Security profile to enable inline cloud analysis (to analyze traffic for command injection and SQL injection vulnerabilities in real-time).
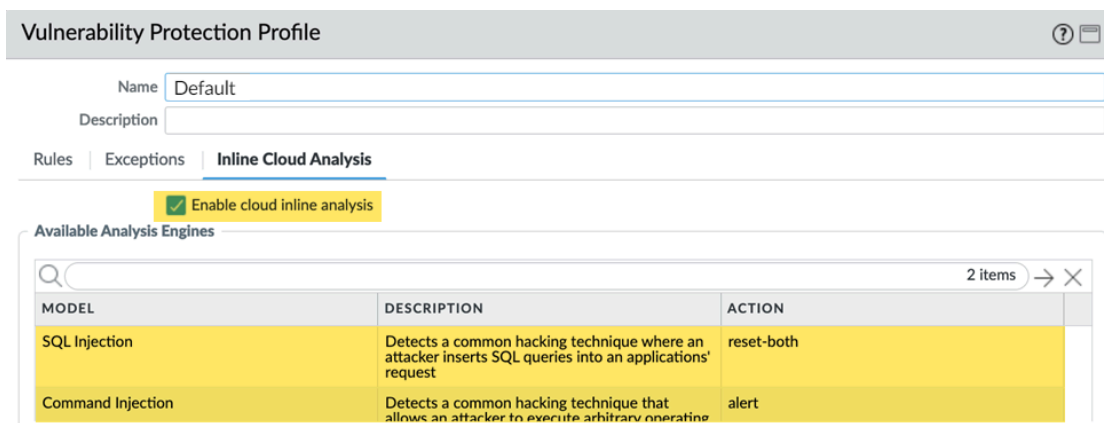
1. Select an existing Vulnerability Protection security profile or **Add** a new one (**Objects** > **Security Profiles** > **Vulnerability Protection**).

2. Select your Vulnerability Protection profile and then go to **Inline Cloud Analysis** and **Enable cloud inline analysis**.

3. Specify an **Action** to take when a vulnerability exploit is detected using a corresponding analysis engine. There are currently two analysis engines available: **SQL Injection** and **Command Injection**.

   - **Allow**—The request is allowed and no log entry is generated.
   - **Alert**—The request is allowed and a Threat log entry is generated.
   - **Reset-Client**—Resets the client-side connection.
   - **Reset-Server**—Resets the server-side connection.
   - **Reset-Both**—Resets the connection on both the client and server ends.

4. Click **OK** to exit the Vulnerability Protection Profile configuration dialog and **Commit** your changes.

STEP 6 | (Optional) Add URL and/or IP address exceptions to your Vulnerability Protection profile if Inline Cloud Analysis produces false-positives. You can add exceptions by specifying an external dynamic list (URL or IP address list types) or an **Addresses** object.

1. Add an **External Dynamic Lists** or [IP] **Addresses** object exception.

2. Select **Objects > Security Profiles > Vulnerability** to return to your Vulnerability Protection profile.

3. Select a Vulnerability profile for which you want to exclude specific URLs and/or IP addresses and then select **Inline Cloud Analysis**.

4. **Add** an **EDL URL** or **IP Address**, depending on the type of exception you want to add, and then select a pre-existing URL or IP address external dynamic list. If none are available,

create a new external dynamic list. For IP address exceptions, you can, optionally, select an **Addresses** object list.

> 📋 *Vulnerability profiles that are configured as **Shared** on Panorama-managed firewalls cannot have IP address objects added to the Inline Cloud Analysis exceptions list.*
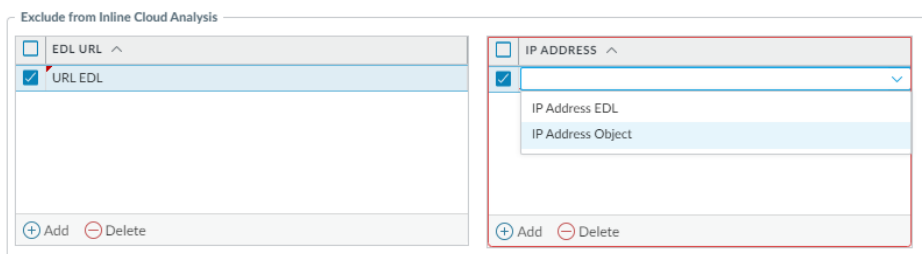
5. Click **OK** to save the Vulnerability Protection profile and **Commit** your changes.

STEP 7 | Configure the timeout latency and action to take when the request exceeds the max latency.

1. Select **Device** > **Setup** > **Content-ID** > **Threat Prevention Inline Cloud Analysis**.

2. Specify the timeout value and the associated action to take when latency limits are reached for Inline Cloud Analysis requests:

   - Max Latency (ms)—Specify the maximum acceptable processing time, in seconds, for Inline Cloud Analysis to return a result.

   - Allow on Max Latency—Enables the firewall to take the action of allow, when the maximum latency is reached. De-selecting this option sets the firewall action to block.

   - Log Traffic Not Scanned— Enables the firewall to log traffic requests that exhibit anomalous traits indicating the presence of advanced and evasive command-and-control (C2) threats, but have not been processed by Threat Prevention Inline Cloud analyzers.

3. Click **OK** to confirm your changes.

STEP 8 | Install a Device Certificate Repeat for all firewalls enabled for inline cloud analysis.

STEP 9 | (Required when the firewall is deployed with an explicit proxy server) Configure the proxy server used to access the servers that facilitate requests generated by all configured inline

cloud analysis features. A single proxy server can be specified and applies to all Palo Alto Networks update services, including all configured inline cloud and logging services.

1. (PAN-OS 11.2.3 and later) Configure the proxy server through PAN-OS.

    1. Select **Device** > **Setup** > **Services** and edit the **Services** details.

    2. Specify the **Proxy Server** settings and **Enable proxy for Inline Cloud Services**. You can provide either an IP address or FQDN in the **Server** field.

        📋 *The proxy server password must contain a minimum of six characters.*

    3. Click **OK**.

2. (PAN-OS 10.2.11 and later) Configure the proxy server through the firewall CLI.

    1. Access the firewall CLI.

    2. Configure the base proxy server settings using the following CLI commands:

```
set deviceconfig system secure-proxy-server <FQDN_or_IP>
set deviceconfig system secure-proxy-port <1-65535>
set deviceconfig system secure-proxy-user <value>
set deviceconfig system secure-proxy-password <value>
```

        📋 *The proxy server password must contain a minimum of six characters.*

    3. Enable the proxy server to send requests to the inline cloud service servers using the following CLI command:

```
debug dataplane mica set inline-cloud-proxy enable
```

    4. View the current operational status of proxy support for inline cloud services using the following CLI command:

```
debug dataplane mica show inline-cloud-proxy
```

        For example:

```
debug dataplane mica show inline-cloud-proxy

Proxy for Advanced Services is Disabled
```

STEP 10 | (Optional) Set the Cloud Content Fully Qualified Domain Name (FQDN) used by the firewall to handle inline cloud analysis service requests. The default FQDN connects to hawkeye.services-edge.paloaltonetworks.com and then resolves to the closest cloud services server. You can override the automatic server selection by specifying a regional cloud content server that best meets your data residency and performance requirements.

📋 *The Cloud Content FQDN is a globally used resource and affects how other services that rely on this connection sends traffic payloads.*

Verify that the firewall uses the correct Content Cloud FQDN (**Device** > **Setup** > **Content-ID** > **Content Cloud Setting**) for your region and change the FQDN if necessary:

📋 *If your NGFW is configured inline to facilitate a SaaS Security deployment, please note that the FQDNs located in France and Japan do not currently support SaaS Security functionality.*

- US Central (Iowa, US)—`us.hawkeye.services-edge.paloaltonetworks.com`
- Europe (Frankfurt, Germany)—`eu.hawkeye.services-edge.paloaltonetworks.com`
- APAC (Singapore)—`apac.hawkeye.services-edge.paloaltonetworks.com`
- India (Mumbai)—`in.hawkeye.services-edge.paloaltonetworks.com`
- UK (London, England)—`uk.hawkeye.services-edge.paloaltonetworks.com`
- France (Paris, France)—`fr.hawkeye.services-edge.paloaltonetworks.com`
- Japan (Tokyo, Japan)—`jp.hawkeye.services-edge.paloaltonetworks.com`
- Australia (Sydney, Australia)—`au.hawkeye.services-edge.paloaltonetworks.com`
- Canada (Montréal, Canada)—`ca.hawkeye.services-edge.paloaltonetworks.com`
- Switzerland (Zürich, Switzerland)—`ch.hawkeye.services-edge.paloaltonetworks.com`

STEP 11 | (Optional) Verify the status of your firewall connectivity to the Advanced Threat Prevention cloud service.

Use the following CLI command on the firewall to view the connection status.

```
show ctd-agent status security-client
```

For example:

```
show ctd-agent status security-client

...
Security Client AceMlc2(1)
Current cloud server:          hawkeye.services-
edge.paloaltonetworks.com
Cloud connection:              connected
```

```
. . .
```

📋 *CLI output shortened for brevity.*

If you are unable to connect to the Advanced Threat Prevention cloud service, verify that the following domain is not being blocked: hawkeye.services-edge.paloaltonetworks.com.

STEP 12 | (Optional) Monitor Advanced Threat Prevention

Configure Inline Cloud Analysis (Strata Cloud Manager)

STEP 1 | To take advantage of inline cloud analysis, you must have an active Prisma Access subscription, which provides access to Advanced Threat Prevention features. For information about the applications and services offered with Prisma Access, refer to All Available Apps and Services.

To verify subscriptions for which you have currently-active licenses, Check What's Supported With Your License.

STEP 2 | Use the credentials associated with your Palo Alto Networks support account and log in to the Strata Cloud Manager on the hub.

STEP 3 | Update or create a new Anti-Spyware Security profile to enable inline cloud analysis (to analyze traffic for advanced C2 (command-and-control) and spyware threats in real-time).

1. Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Anti-Spyware**.

2. Select your Anti-Spyware security profile and then go to **Inline Cloud Analysis** panel and **Enable Inline Cloud Analysis**.

Inline Cloud Analysis

☑ Enable Inline Cloud Analysis

Available Analysis Engines

Model	Description	Action Setting
HTTP Command and Control detector	Machine Learning engine to detect HTTP based command and control traffic	alert
HTTP2 Command and Control detector	Machine Learning engine to detect HTTP2 based command and control traffic	alert
SSL Command and Control detector	Machine Learning engine to detect SSL based command and control traffic	alert
Unknown-TCP Command and Control detector	Machine Learning engine to detect Unknown-TCP based command and control traffic	alert

3. Specify an **Action** to take when a threat is detected using a corresponding analysis engine.

> 📋 *The default action for each analysis engine is **alert**, however, Palo Alto Networks recommends setting all actions to **Reset-Both** for the best security posture.*

- **Allow**—The request is allowed and no log entry is generated.

- **Alert**—The request is allowed and a Threat log entry is generated.

- **Drop**—Drops the request; a reset action is not sent to the host/application.

- **Reset-Client**—Resets the client-side connection.

- **Reset-Server**—Resets the server-side connection.

- **Reset-Both**—Resets the connection on both the client and server ends.

4. Click **OK** to exit the Anti-Spyware Profile configuration dialog and **Commit** your changes.

STEP 4 | (Optional) Add URL and/or IP address exceptions to your Anti-Spyware profile if Inline Cloud Analysis produces false-positives. You can add exceptions by specifying an external dynamic list (URL or IP address list types) or an **Addresses** policy object.

1. Add an **External Dynamic Lists** or [IP] **Addresses** object exception.

2. Select **Manage** > **Configuration** > **Anti-Spyware**.

3. Select an Anti-Spyware profile for which you want to exclude specific URLs and/or IP addresses and then go to the **Inline Cloud Analysis** pane.

4. **Add EDL/URL** or **Add IP Address**, depending on the type of exception you want to add, and then select a pre-existing URL or IP address external dynamic list. If none are available,

create a new external dynamic list policy object. For IP address exceptions, you can, optionally, select an **Addresses** object list.

Exceptions - EDL/URLs (0)	Delete	Add EDL/URL
☐ EDL/URL		
No EDLs or URLs.		

Exceptions - IP Addresses (0)	Delete	Add IP Address
☐ IP Address		
No IP Addresses.		

5. Click **OK** to save the Anti-Spyware profile and **Commit** your changes.

STEP 5 | (Optional) Monitor Advanced Threat Prevention

Prevent Brute Force Attacks

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

A brute force attack uses a large volume of requests/responses from the same source or destination IP address to break into a system. The attacker employs a trial-and-error method to guess the response to a challenge or a request.

The Vulnerability Protection profile includes signatures to protect against brute force attacks. Each signature has an ID, Threat Name, and Severity and is triggered when a pattern is recorded. The pattern specifies the conditions and interval at which the traffic is identified as a brute-force attack; some signatures are associated with another child signature that is of a lower severity and specifies the pattern to match against. When a pattern matches against the signature or child signature, it triggers the default action for the signature.

To enforce protection:

• Attach the Vulnerability Protection profile to a Security policy rule. See Set Up Antivirus, Anti-Spyware, and Vulnerability Protection.

• Install content updates that include new signatures to protect against emerging threats for the firewall. See Install Content and Software Updates.

Customize the Action and Trigger Conditions for a Brute Force Signature

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

The firewall includes two types of predefined brute force signatures—parent signatures and child signatures. A child signature is a single occurrence of a traffic pattern that matches the signature. A parent signature is associated with a child signature and is triggered when multiple events occur within a specified time interval and that matches the traffic pattern defined in the child signature.

Typically, the default action for a child signature is *allow* because a single event is not indicative of an attack. This ensures that legitimate traffic is not blocked and avoids generating threat logs for non-noteworthy events. Palo Alto Networks recommends that you do not change the default action without careful consideration.

In most cases, the brute force signature is a noteworthy event due to its recurrent pattern. If needed, you can do one of the following to customize the action for a brute-force signature:

• Create a rule to modify the default action for all signatures in the brute force category. You can choose to allow, alert, block, reset, or drop the traffic.

• Define an exception for a specific signature. For example, you can search for and define an exception for a CVE.

For a parent signature, you can modify both the trigger conditions and the action; for a child signature, you can modify only the action.

> *To effectively mitigate an attack, specify the block-ip address action instead of the drop or reset action for most brute force signatures.*

STEP 1 | Create a new Vulnerability Protection profile.

1. Select **Objects** > **Security Profiles** > **Vulnerability Protection** and **Add** a profile.
2. Enter a **Name** for the Vulnerability Protection profile.
3. (Optional) Enter a **Description**.
4. (Optional) Specify that the profile is **Shared** with:

   • **Every virtual system (vsys) on a multi-vsys firewall**—If cleared (disabled), the profile is available only to the Virtual System selected in the **Objects** tab.

   • **Every device group on Panorama**—If cleared (disabled), the profile is available only to the Device Group selected in the **Objects** tab.

5. (Optional—Panorama only) Select **Disable override** to prevent administrators from overriding the settings of this Vulnerability Protection profile in device groups that

inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.

STEP 2 | Create a rule that defines the action for all signatures in a category.

1. On the **Rules** tab, **Add** and enter a **Rule Name** for a new rule.

2. (Optional) Specify a specific threat name (default is **any**).

3. Set the **Action**. In this example, it is set to **Block IP**.

    > *If you set a Vulnerability Protection profile to Block IP, the firewall first uses hardware to block IP addresses. If attack traffic exceeds the blocking capacity of the hardware, the firewall then uses software blocking mechanisms to block the remaining IP addresses.*

4. Set **Category** to **brute-force**.

5. (Optional) If blocking, specify the **Host Type** on which to block: **server** or **client** (default is **any**).

6. See Step 3 to customize the action for a specific signature.

7. See Step 4 to customize the trigger threshold for a parent signature.

8. Click **OK** to save the rule and the profile.

STEP 3 | (Optional) Customize the action for a specific signature.

1. On the **Exceptions** tab, **Show all signatures** to find the signature you want to modify.

    To view all the signatures in the brute-force category, search for `category contains 'brute-force'`.

2. To edit a specific signature, click the predefined default action in the Action column.

Vulnerability Protection Profile | | | | | | | | | | ⑦ ▭ |

Name | Modify-brute-force-rule

Description | any

☐ Shared

Rules | **Exceptions**

🔍 category contains "brute-force"   138 / 15016 → ✕

ENAB...	ID	THREAT NAME	IP ADDRESS EXEMPTI...	RULE	CVE	HOST	CATEGORY	SEVERI...	ACTION	PACKET CAPTURE
☐	39...	HTTP Request Brute Force Attack				server	brute-force	informa...	default (allow)	disable
☐	31...	Microsoft Communicator INVITE Flood Denial of Service Vulnerability			CVE-2008-5180	server	brute-force	informa...	default (allow)	disable
☐	34...	SIP Bye Request Attempt				server	brute-force	informa...	default (allow)	disable
☐	33...	SIP Register Request Attempt				server	brute-force	informa...	default (allow)	disable
☐	31...	Telnet Authentication Failed				server	brute-force	informa...	default (allow)	disable

✅ Show all signatures   📄 PDF/CSV   ⏮ ◂ | Page 1 of 5 | ▸ ⏭ | ↻ Displaying 1 - 30/ 138 threats

3. Set the action: **Allow**, **Alert**, **Block Ip**, or **Drop**. If you select **Block Ip**, complete these additional tasks:

    1. Specify the **Time** period (in seconds) after which to trigger the action.

    2. Specify whether to **Track By** and block the IP address using the **IP source** or the **IP source and destination**.

4. Click **OK**.

5. For each modified signature, select the check box in the **Enable** column.

6. Click **OK**.

STEP 4 | Customize the trigger conditions for a parent signature.

A parent signature that can be edited is marked with this icon: ▨ .

In this example, the search criteria was brute force category and CVE-2008-1447.

1. Edit (▨) the time attribute and the aggregation criteria for the signature.

2. To modify the trigger threshold, specify the **Number of Hits** per number of **seconds**.

3. Specify whether to aggregate the number of hits (**Aggregation Criteria**) by **source**, **destination**, or **source-and-destination**.

4. Click **OK**.

STEP 5 | Attach this new profile to a Security policy rule.

1. Select **Policies** > **Security** and **Add** or modify a Security policy rule.
2. On the **Actions** tab, select **Profiles** as the **Profile Type** for the Profile Setting.
3. Select your **Vulnerability Protection** profile.
4. Click **OK**.

STEP 6 | Commit your changes.

1. Click **Commit**.

Enable Evasion Signatures

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Palo Alto Networks evasion signatures detect crafted HTTP or TLS requests, and can alert to instances where a client connects to a domain other than the domain specified in a DNS query. Evasion signatures are effective only when the firewall is also enabled to act as a DNS proxy and resolve domain name queries. As a best practice, take the following steps to enable evasion signatures.

STEP 1 | Enable a firewall intermediate to clients and servers to act as a DNS proxy.

Configure a DNS Proxy Object, including:

- Specify the interfaces on which you want the firewall to listen for DNS queries.
- Define the DNS servers with which the firewall communicates to resolve DNS requests.
- Set up static FQDN-to-IP address entries that the firewall can resolve locally, without reaching out to DNS servers.
- Enable caching for resolved hostname-to-IP-address mappings.

STEP 2 | Get the latest Applications and Threats content version (at least content version 579 or later).

1. Select **Device** > **Dynamic Updates**.
2. **Check Now** to get the latest Applications and Threats content update.
3. Download and Install Applications and Threats content version 579 (or later).

STEP 3 | Define how the firewall should enforce traffic matched to evasion signatures.

1. Select **Objects** > **Security Profiles** > **Anti-Spyware** and **Add** or modify an Anti-spyware profile.
2. Select **Exceptions** and select **Show all signatures**.
3. Filter signatures based on the keyword `evasion`.
4. For all evasion signatures, set the **Action** to any setting other than allow or the default action (the default action is for evasion signatures is allow). For example, set the **Action** for signature IDs 14978 and 14984 to **alert** or **drop**.
5. Click **OK** to save the updated Anti-spyware profile.
6. Attach the Anti-spyware profile to a security policy rule: Select **Policies** > **Security**, select the desired policy to modify and then click the **Actions** tab. In Profile Settings, click the drop-down next to **Anti-Spyware** and select the anti-spyware profile you just modified to enforce evasion signatures.

STEP 4 | Commit your changes.

Click **Commit**.

Create Threat Exceptions

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Palo Alto Networks defines a recommended default action (such as block or alert) for threat signatures. You can use a threat ID to exclude a threat signature from enforcement or modify the action that is enforced for that threat signature. For example, you can modify the action for threat signatures that are triggering false positives on your network.

Configure threat exceptions for antivirus, vulnerability, spyware, and DNS signatures to change enforcement for a threat. However, before you begin, make sure the threats are being properly detected and enforced based on the default or best practice signature settings for an optimum security posture:

- Get the latest Antivirus, Threats and Applications, and WildFire signature updates (for the firewall).
- Set Up Antivirus, Anti-Spyware, and Vulnerability Protection and apply these security profiles to your security policy.
- Strata Cloud Manager
- PAN-OS & Panorama

Create Threat Exceptions (Strata Cloud Manager)

STEP 1 | Exclude antivirus signatures from enforcement.

> 📋 *While you can use an WildFire and Antivirus profile to exclude antivirus signatures from enforcement, you cannot change the action is enforced for a specific antivirus signature. However, you can define the enforceable action when viruses are found in different types of traffic by editing the security profile **Enforcement Actions**.*

1. Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **WildFire and Antivirus**.

2. **Add Profile** or select an existing WildFire and Antivirus profile from which you want to exclude a threat signature and go to the **Advanced Settings** tab.

3. From the **Signature Exceptions** menu, **Add Exception** and provide the **Threat ID** for the threat signature you want to exclude from enforcement. You can optionally add notes to the signature exception.

4. **Save** the signature exception when you are finished.

5. A valid threat signature ID auto-populates the threat name field. You can view a complete list of active signature exceptions as well as **Delete** entries that are no longer necessary.

6. Repeat to add additional exceptions or click **Save** after all of your threat exceptions have been added.

STEP 2 | Modify enforcement for vulnerability and spyware signatures (except DNS signatures; while they are a type of spyware signature, DNS signatures are handled through the DNS Security subscription in Prisma Access).

1. Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Anti-Spyware** or **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Vulnerability Protection**, depending upon the signature type.

2. **Add Profile** or select an existing Anti-Spyware or Vulnerability Protection profile from which you want to modify the signature enforcement, and then select **Add Override**.

3. Search for spyware or vulnerability signatures by providing the relevant **Match Criteria**. This automatically filters the available signatures and displays the results in the **Matching Signatures** section.

4. Select the check box for the signature(s) whose enforcement you want to modify.

5. Provide the updated **Action**, **Packet Capture**, and **IP Addresses** that you want the modified enforcement rules to apply to for the selected signatures.

Overrides

Exclude a signature from enforcement or change a signature action by creating an override (exception). Only override the default behaviour for a signature if you know that the activity the signature detects does not pose a threat to your organization.

If you think you've identified a false positive, open a support case so that the Palo Alto Networks threat team can investigate. When the issue is resolved, remove the corresponding override.

Match Criteria   Clear Filters

Severity	Category		Threat Name
any	dns-security		any
critical	dns-wildfire		
high	domain-edl		Threat ID ⓘ
informational	downloader		any
low	fraud		
medium	hacktool		
	inline-cloud-c2		
	keylogger		
	net-worm		
	p2p-communication		

Matching Signatures (22/8588)   🔍 Search by string, CVE or threat ID   Page 1 of 2 < >

☐	Threat Name	Threat ID	Category	Severity	Default Action
☑	CoinHive Site Detection	85692	fraud	critical	reset-both
☑	CoinHive Site Detection	85695	fraud	critical	reset-both
☑	CoinHive Site Detection	85696	fraud	critical	reset-both
☑	CoinHive Site Detection	85697	fraud	critical	reset-both
☐	Skimmer Site Detection	85812	fraud	critical	reset-both
☐	Skimmer Site Detection	85826	fraud	critical	reset-both

Action
Allow ▾

Packet Capture
disable ✕ ▾

Notes

Apply to IP Addresses

IP Addresses (1)   🔍 Search   Delete   Add IP Addresses

☑	IP
☑	1.1.1.1

Enter valid unicast IP Address (e.g. 10.1.7.8 or 2001:db8:123:1::1)

∗ Required Field   Cancel   Save

6. **Save** your updated signature enforcement configuration.

7. You can view a complete list of **Overrides** including various statistics, as well as **Delete** entries that are no longer necessary.

Overrides (4)

Exclude a signature from enforcement or change the signature action. You can limit threat overrides based on IP address, where the override applies only when an IP address is the source or destination for a session.   Delete   Add Override

|	Threat ID	Threat Name	Severity	Category	Applied to IP Addr...	Hits (7 Days)	Last Triggered
☐	85692	CoinHive Site Detection	critical	fraud	1.1.1.1	0	0
☐	85695	CoinHive Site Detection	critical	fraud	1.1.1.1	0	0
☐	85696	CoinHive Site Detection	critical	fraud	1.1.1.1	0	0
☐	85697	CoinHive Site Detection	critical	fraud	1.1.1.1	0	0

Create Threat Exceptions (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | Exclude antivirus signatures from enforcement.

> *While you can use an Antivirus profile to exclude antivirus signatures from enforcement, you cannot change the action the firewall enforces for a specific antivirus signature. However, you can define the action for the firewall to enforce for viruses found in different types of traffic by editing the Decoders (**Objects** > **Security Profiles** > **Antivirus** > **<antivirus-profile>** > **Antivirus**).*

1. Select **Objects** > **Security Profiles** > **Antivirus**.
2. **Add** or modify an existing Antivirus profile from which you want to exclude a threat signature and select **Signature Exceptions**.
3. **Add** the **Threat ID** for the threat signature you want to exclude from enforcement.
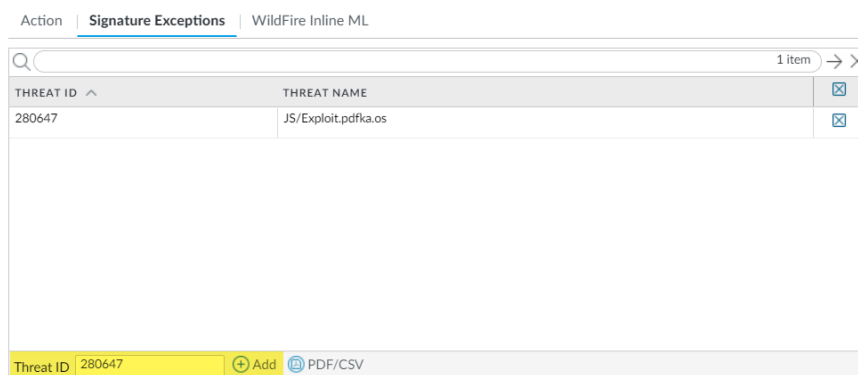
4. Click **OK** to save the Antivirus profile.

STEP 2 | Modify enforcement for vulnerability and spyware signatures (except DNS signatures; skip to the next option to modify enforcement for DNS signatures, which are a type of spyware signature).

1. Select **Objects** > **Security Profiles** > **Anti-Spyware** or **Objects** > **Security Profiles** > **Vulnerability Protection**.

2. **Add** or modify an existing Anti-Spyware or Vulnerability Protection profile from which you want to exclude the threat signature and then select either **Signature Exceptions** for Anti-Spyware Protection profiles or **Exceptions** for Vulnerability Protection profiles.

3. **Show all signatures** and then filter to select the signature for which you want to modify enforcement rules.

4. Check the box under the **Enable** column for the signature whose enforcement you want to modify.

5. Select the **Action** you want the firewall to enforce for this threat signature.
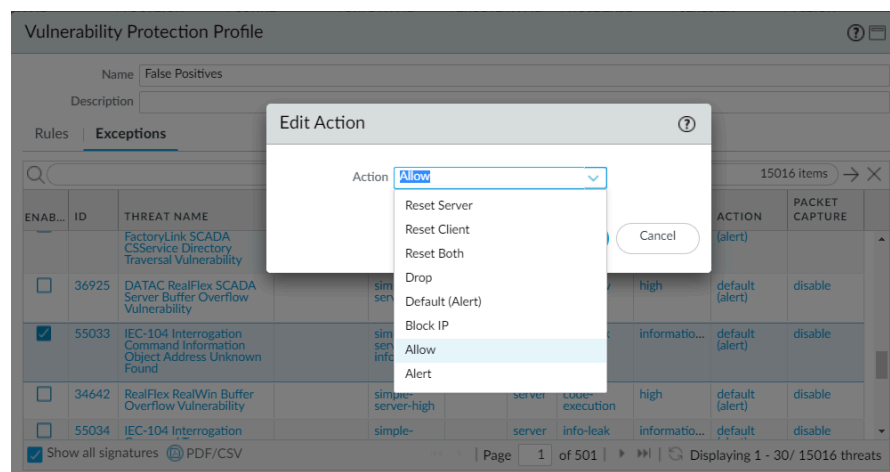
For signatures that you want to exclude from enforcement because they trigger false positives, set the **Action** to **Allow**.

6. Click **OK** to save your new or modified Anti-Spyware or Vulnerability Protection profile.

STEP 3 | Modify enforcement for DNS signatures.

By default, the DNS lookups to malicious hostnames that DNS signatures are detect are sinkholed.

1. Select **Objects** > **Security Profiles** > **Anti-Spyware**.

2. **Add** or modify the Anti-Spyware profile from which you want to exclude the threat signature, and select **DNS Exceptions**.

3. Search for the DNS Threat ID for the DNS signature that you want to exclude from enforcement and select the box of the applicable signature:
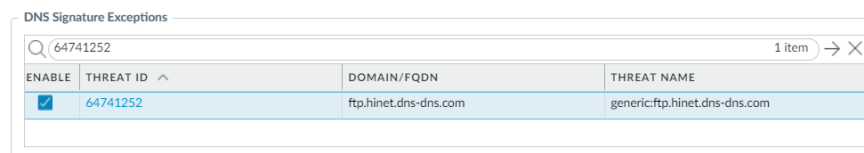
4. Click **OK** to save your new or modified Anti-Spyware profile.

Use DNS Queries to Identify Infected Hosts on the Network

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

The DNS sinkhole action in Anti-Spyware profiles enables the firewall to forge a response to a DNS query for a known malicious domain or to a custom domain, so that you can identify hosts on your network that have been infected with malware. A compromised host might initiate communication with a command-and-control (C2) server—once the connection is made, an attacker can remotely control the infected host, in order to further infiltrate the network or exfiltrate data.

DNS queries to any domain included in the Palo Alto Networks DNS signatures list is sinkholed to a Palo Alto Networks server IP address.

The firewall has two sources of DNS signatures that it can use to identify malicious and C2 domains:

- (Requires an Advanced | Threat Prevention subscription) Local DNS signatures—This is a limited, on-box set of DNS signatures that the firewall can use to identify malicious domains. The firewall gets new DNS signatures as part of daily antivirus updates.

- (Requires a DNS Security subscription) DNS Security signatures—The firewall accesses the Palo Alto Networks DNS Security cloud service to check for malicious domains against the complete database of DNS signatures. Certain signatures—that only DNS Security provides—can uniquely detect C2 attacks that use machine learning techniques, like domain generation algorithms (DGAs) and DNS tunneling. For more information about the DNS Security subscription, refer to the DNS Security guide.

  If you want to specify a sinkhole action for DNS Security signatures, you can configure those settings as part of your DNS Security profile.

DNS queries to domains in the local DNS signature set or the DNS Security signature set are redirected to a Palo Alto Networks server, and the host is unable to access the malicious domain. The following topics provide details on how to enable DNS sinkholing so that you can identify infected hosts.

- How DNS Sinkholing Works
- Configure DNS Sinkholing
- Configure DNS Sinkholing for a List of Custom Domains
- Configure the Sinkhole IP Address to a Local Server on Your Network
- See Infected Hosts that Attempted to Connect to a Malicious Domain

How DNS Sinkholing Works

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

DNS sinkholing helps you to identify infected hosts on the protected network using DNS traffic in situations where the firewall cannot see the infected client's DNS query (that is, the firewall cannot see the originator of the DNS query). In a typical deployment where the firewall is north of the local DNS server, the threat log will identify the local DNS resolver as the source of the traffic rather than the actual infected host. Sinkholing malware DNS queries solves this visibility problem by forging responses to the client host queries directed at malicious domains, so that clients attempting to connect to malicious domains (for command-and-control, for example) will instead attempt to connect to a default Palo Alto Networks sinkhole IP address (or to IP address that you define if you choose to Configure DNS Sinkholing for a List of Custom Domains). Infected hosts can then be easily identified in the traffic logs.

1. Botnet on client host 192.168.2.10 sends DNS query for Hacker Server (malicious domain).
2. The internal DNS server relays the request through the firewall to the public DNS server.
3. The firewall queries the configured DNS signature source and detects the malicious domain request and forges the DNS reply with the sinkhole IP addresses (IPv4 and IPv6).
4. Botnet then attempts to communicate with Hacker Server, but sends to the sinkhole IP address instead.
5. Session goes through the firewall from the user to the sinkhole address.
6. The security admin can then identify all client hosts trying to communicate with the sinkhole IP address by searching for the sinkhole IP address in the threat and traffic logs.
7. The Helpdesk then eradicates the botnet from all infected hosts.

Note: The client hosts and sinkhole IP must be in different zones, so sessions pass through the firewall. The sinkhole IP address does not have to be an active host, just an unused IP address.

Hacker Server

Public DNS Server

Router

Untrust Zone

DNS Signature Source
• Content DNS Signatures: Locally-accessed signatures
• DNS Security: Cloud-accessed signatures

Firewall

Trust Zone

Switch

Internal DNS Server

Desktop
192.168.2.10

Configure DNS Sinkholing

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

To enable DNS sinkholing, attach the default Anti-Spyware profile to a firewall security policy rule (see Set Up Antivirus, Anti-Spyware, and Vulnerability Protection). DNS queries to any domain included in the Palo Alto Networks DNS signature source that you specify are resolved to the default Palo Alto Networks sinkhole IP address. The IP addresses currently are IPv4— sinkhole.paloaltonetworks.com and a loopback address IPv6 address—::1. These address are subject to change and can be updated with content updates.

STEP 1 | Enable DNS sinkholing for the custom list of domains in an external dynamic list.

1. Select **Objects** > **Security Profiles** > **Anti-Spyware**.
2. Modify an existing profile, or select one of the existing default profiles and clone it.
3. **Name** the profile and select the **DNS Policies** tab.
4. Verify that **default-paloalto-dns** is present in the **Signature Source**.
5. (Optional) In the **Packet Capture** drop-down, select **single-packet** to capture the first packet of the session or **extended-capture** to set between 1-50 packets. You can then use the packet captures for further analysis.

STEP 2 | Verify the sinkholing settings on the Anti-Spyware profile.

1. On the **DNS Policies** tab, verify that the **Policy Action** on DNS queries is **sinkhole**.
2. In the DNS Sinkhole Settings section, verify that **Sinkhole** is enabled. For your convenience, the default Sinkhole IP address is set to access a Palo Alto Networks server. Palo Alto Networks can automatically refresh this IP address through content updates.

   If you want to modify the **Sinkhole IPv4** or **Sinkhole IPv6** address to a local server on your network or to a loopback address, see Configure the Sinkhole IP Address to a Local Server on Your Network.
3. Click **OK** to save the Anti-Spyware profile.

STEP 3 | Attach the Anti-Spyware profile to a Security policy rule.

1. Select **Policies** > **Security** and select a security policy rule.
2. On the **Actions** tab, select the **Log at Session Start** check box to enable logging.
3. In the Profile Setting section, click the **Profile Type** drop-down to view all **Profiles**. From the **Anti-Spyware** drop-down and select the new profile.
4. Click **OK** to save the policy rule.

STEP 4 | Test that the policy action is enforced by monitoring the activity on the firewall.

1. Select **ACC** and add a URL Domain as a global filter to view the Threat Activity and Blocked Activity for the domain you accessed.

2. Select **Monitor** > **Logs** > **Threat** and filter by `(action eq sinkhole)` to view logs on sinkholed domains.

Configure DNS Sinkholing for a List of Custom Domains

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

To enable DNS Sinkholing for a custom list of domains, you must create an External Dynamic List that includes the domains, enable the sinkhole action in an Anti-Spyware profile and attach the profile to a security policy rule. When a client attempts to access a malicious domain in the list, the firewall forges the destination IP address in the packet to the default Palo Alto Networks server or to a user-defined IP address for sinkholing.

For each custom domain included in the external dynamic list, the firewall generates DNS-based spyware signatures. The signature is named Custom Malicious DNS Query <domain name>, and is of type spyware with medium severity; each signature is a 24-byte hash of the domain name.

For information about the domain list entry limits, refer to External Dynamic List.

STEP 1 | Enable DNS sinkholing for the custom list of domains in an external dynamic list.

1. Select **Objects** > **Security Profiles** > **Anti-Spyware**.

2. Modify an existing profile, or select one of the existing default profiles and clone it.

3. **Name** the profile and select the **DNS Policies** tab.

4. Select an EDL from the **External Dynamic Lists** signature source.

   ⊖ *If you have already created an external dynamic list of type: **Domain List**, you can select it from here. The list does not display external dynamic lists of type URL or IP Address that you may have created.*

5. Configure the external dynamic list from the Anti-Spyware profile (see Configure the Firewall to Access an External Dynamic List). The **Type** is preset to **Domain List**.

6. (Optional) In the **Packet Capture** drop-down, select **single-packet** to capture the first packet of the session or **extended-capture** to set between 1-50 packets. You can then use the packet captures for further analysis.

STEP 2 | Verify the sinkholing settings on the Anti-Spyware profile.

1. On the **DNS Policies** tab, verify that the **Policy Action** on DNS queries is **sinkhole**.

2. In the DNS Sinkhole Settings section, verify that **Sinkhole** is enabled. For your convenience, the default Sinkhole IP address is set to access a Palo Alto Networks

server. Palo Alto Networks can automatically refresh this IP address through content updates.

If you want to modify the **Sinkhole IPv4** or **Sinkhole IPv6** address to a local server on your network or to a loopback address, see Configure the Sinkhole IP Address to a Local Server on Your Network.

3. Click **OK** to save the Anti-Spyware profile.

STEP 3 | Attach the Anti-Spyware profile to a Security policy rule.

1. Select **Policies** > **Security** and select a security policy rule.
2. On the **Actions** tab, select the **Log at Session Start** check box to enable logging.
3. In the Profile Setting section, click the **Profile Type** drop-down to view all **Profiles**. From the **Anti-Spyware** drop-down and select the new profile.
4. Click **OK** to save the policy rule.

STEP 4 | Test that the policy action is enforced.

1. View External Dynamic List Entries that belong to the domain list, and access a domain from the list.
2. To monitor the activity on the firewall:

   1. Select **ACC** and add a URL Domain as a global filter to view the Threat Activity and Blocked Activity for the domain you accessed.
   2. Select **Monitor** > **Logs** > **Threat** and filter by (`action eq sinkhole`) to view logs on sinkholed domains.

STEP 5 | Verify whether entries in the external dynamic list are ignored or skipped.

Use the following CLI command on the firewall to review the details about the list.

```
request system external-list show type domain name <list_name>
```

For example:

```
request system external-list show type domain name
My_List_of_Domains_2015
vsys1/EBLDomain:
Next update at : Thu May 21 10:15:39 2015
Source : https://1.2.3.4/My_List_of_Domains_2015
Referenced : Yes
Valid : Yes
Number of entries : 3
```

```
domains:www.example.com
baddomain.com
qqq.abcedfg.com
```

STEP 6 | (Optional) Retrieve the external dynamic list on-demand.

To force the firewall to retrieve the updated list on-demand instead of at the next refresh interval (the **Repeat** frequency you defined for the external dynamic list), use the following CLI command:

```
request system external-list refresh type domain name  <list_name>
```

💡 *As an alternative, you can use the firewall interface to* Retrieve an External Dynamic List from the Web Server.

Configure the Sinkhole IP Address to a Local Server on Your Network

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

By default, sinkholing is enabled for all Palo Alto Networks DNS signatures, and the sinkhole IP address is set to access a Palo Alto Networks server. Use the instructions in this section if you want to set the sinkhole IP address to a local server on your network.

You must obtain both an IPv4 and IPv6 address to use as the sinkhole IP addresses because malicious software may perform DNS queries using one or both of these protocols. The DNS sinkhole address must be in a different zone than the client hosts to ensure that when an infected host attempts to start a session with the sinkhole IP address, it will be routed through the firewall.

⊖ *The sinkhole addresses must be reserved for this purpose and do not need to be assigned to a physical host. You can optionally use a honey-pot server as a physical host to further analyze the malicious traffic.*

The configuration steps that follow use the following example DNS sinkhole addresses:

IPv4 DNS sinkhole address—10.15.0.20

IPv6 DNS sinkhole address—fd97:3dec:4d27:e37c:5:5:5:5

STEP 1 | Configure the sinkhole interface and zone.

Traffic from the zone where the client hosts reside must route to the zone where the sinkhole IP address is defined, so traffic will be logged.

Use a dedicated zone for sinkhole traffic, because the infected host will be sending traffic to this zone.

1. Select **Network** > **Interfaces** and select an interface to configure as your sinkhole interface.
2. In the **Interface Type** drop-down, select **Layer3**.
3. To add an IPv4 address, select the **IPv4** tab and select **Static** and then click **Add**. In this example, add 10.15.0.20 as the IPv4 DNS sinkhole address.
4. Select the **IPv6** tab and click **Static** and then click **Add** and enter an IPv6 address and subnet mask. In this example, enter fd97:3dec:4d27:e37c::/64 as the IPv6 sinkhole address.
5. Click **OK** to save.
6. To add a zone for the sinkhole, select **Network** > **Zones** and click **Add**.
7. Enter zone **Name**.
8. In the **Type** drop-down select **Layer3**.
9. In the **Interfaces** section, click **Add** and add the interface you just configured.
10. Click **OK**.

STEP 2 | Enable DNS sinkholing.

By default, sinkholing is enabled for all Palo Alto Networks DNS signatures. To change the sinkhole address to your local server, see Step 2 in Configure DNS Sinkholing for a List of Custom Domains.

STEP 3 | Edit the security policy rule that allows traffic from client hosts in the trust zone to the untrust zone to include the sinkhole zone as a destination and attach the Anti-Spyware profile.

Editing the Security policy rule(s) that allows traffic from client hosts in the trust zone to the untrust zone ensures that you are identifying traffic from infected hosts. By adding the sinkhole zone as a destination on the rule, you enable infected clients to send bogus DNS queries to the DNS sinkhole.

1. Select **Policies** > **Security**.
2. Select an existing rule that allows traffic from the client host zone to the untrust zone.
3. On the **Destination** tab, **Add** the Sinkhole zone. This allows client host traffic to flow to the sinkhole zone.
4. On the **Actions** tab, select the **Log at Session Start** check box to enable logging. This will ensure that traffic from client hosts in the Trust zone will be logged when accessing the Untrust or Sinkhole zones.
5. In the **Profile Setting** section, select the **Anti-Spyware** profile in which you enabled DNS sinkholing.
6. Click **OK** to save the Security policy rule and then **Commit**.

STEP 4 | To confirm that you will be able to identify infected hosts, verify that traffic going from the client host in the Trust zone to the new Sinkhole zone is being logged.

In this example, the infected client host is 192.168.2.10 and the Sinkhole IPv4 address is 10.15.0.20.

1.   From a client host in the trust zone, open a command prompt and run the following command:

```
C:\>ping <sinkhole address>
```

The following example output shows the ping request to the DNS sinkhole address at 10.15.0.2 and the result, which is `Request timed out` because in this example the sinkhole IP address is not assigned to a physical host:

```
C:\>ping 10.15.0.20
Pinging 10.15.0.20 with 32 bytes of data:
Request timed out.
Request timed out.
Ping statistics for 10.15.0.20:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

2.   On the firewall, select **Monitor** > **Logs** > **Traffic** and find the log entry with the Source 192.168.2.10 and Destination 10.15.0.20. This will confirm that the traffic to the sinkhole IP address is traversing the firewall zones.

> 💡 *You can search and/or filter the logs and only show logs with the destination 10.15.0.20. To do this, click the IP address (10.15.0.20) in the **Destination** column, which will add the filter (addr.dst in 10.15.0.20) to the search field. Click the Apply Filter icon to the right of the search field to apply the filter.*

STEP 5 | Test that DNS sinkholing is configured properly.

You are simulating the action that an infected client host would perform when a malicious application attempts to call home.

1.   Find a malicious domain that is included in the firewall's current Antivirus signature database to test sinkholing.

   1.   Select **Device** > **Dynamic Updates** and in the **Antivirus** section click the **Release Notes** link for the currently installed antivirus database. You can also find the antivirus release notes that list the incremental signature updates under Dynamic Updates on the Palo Alto Networks support site.

   2.   In the second column of the release note, locate a line item with a domain extension (for example, .com, .edu, or .net). The left column will display the domain name. For example, Antivirus release 1117-1560, includes an item in the left column named "tbsbana" and the right column lists "net".

      The following shows the content in the release note for this line item:

```
conficker:tbsbana 1
```

```
        variants: net
```

2. From the client host, open a command prompt.

3. Perform an NSLOOKUP to a URL that you identified as a known malicious domain.

    For example, using the URL `track.bidtrk.com`:

    ```
    C:\>nslookup
    track.bidtrk.com
    Server: my-local-dns.local
    Address: 10.0.0.222
    Non-authoritative answer:
    Name: track.bidtrk.com.org
    Addresses: fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
    ```

    In the output, note that the NSLOOKUP to the malicious domain has been forged using the sinkhole IP addresses that we configured (10.15.0.20). Because the domain matched a malicious DNS signature, the sinkhole action was performed.

4. Select **Monitor** > **Logs** > **Threat** and locate the corresponding threat log entry to verify that the correct action was taken on the NSLOOKUP request.

5. Perform a ping to **track.bidtrk.com**, which will generate network traffic to the sinkhole address.

See Infected Hosts that Attempted to Connect to a Malicious Domain

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

After you have configured DNS sinkholing and verified that traffic to a malicious domain goes to the sinkhole address, you should regularly monitor traffic to the sinkhole address, so that you can track down the infected hosts and eliminate the threat.

- Use App Scope to identify infected client hosts.
    1. Select **Monitor** > **App Scope** and select **Threat Monitor**.
    2. Click the **Show spyware** button along the top of the display page.
    3. Select a time range.

        The following screenshot shows three instances of Suspicious DNS queries, which were generated when the test client host performed an NSLOOKUP on a known malicious domain. Click the graph to see more details about the event.
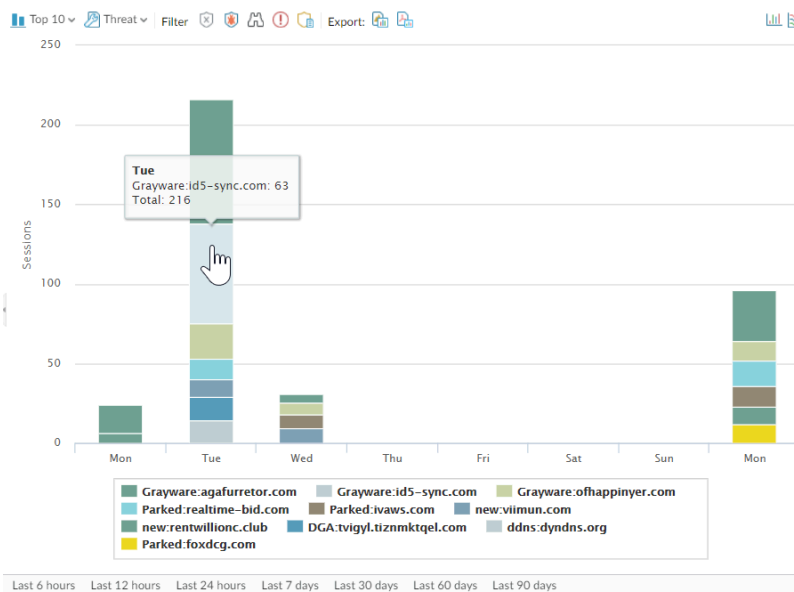
- Configure a custom report to identify all client hosts that have sent traffic to the sinkhole IP address, which is 10.15.0.20 in this example.

    💡 *Forward to an SNMP manager, Syslog server and/or Panorama to enable alerts on these events.*

    In this example, the infected client host performed an NSLOOKUP to a known malicious domain that is listed in the Palo Alto Networks DNS Signature database. When this occurred, the query was sent to the local DNS server, which then forwarded the request through the firewall to an external DNS server. The firewall security policy with the Anti-Spyware profile configured matched the query to the DNS Signature database, which then forged the reply using the sinkhole address of 10.15.0.20 and fd97:3dec:4d27:e37c:5:5:5:5. The client attempts to start a session and the traffic log records the activity with the source host and the destination address, which is now directed to the forged sinkhole address.

    Viewing the traffic log on the firewall allows you to identify any client host that is sending traffic to the sinkhole address. In this example, the logs show that the source address 192.168.2.10 sent the malicious DNS query. The host can then be found and cleaned. Without the DNS sinkhole option, the administrator would only see the local DNS server as the system that performed the query and would not see the client host that is infected. If you attempted

to run a report on the threat log using the action "Sinkhole", the log would show the local DNS server, not the infected host.

1. Select **Monitor** > **Manage Custom Reports**.
2. Click **Add** and **Name** the report.
3. Define a custom report that captures traffic to the sinkhole address as follows:

   - **Database**—Select **Traffic Log**.
   - **Scheduled**—Enable **Scheduled** and the report will run every night.
   - **Time Frame**—30 days
   - **Selected Columns**—Select **Source address** or **Source User** (if you have User-ID configured), which will identify the infected client host in the report, and **Destination address**, which will be the sinkhole address.
   - In the section at the bottom of the screen, create a custom query for traffic to the sinkhole address (10.15.0.20 in this example). You can either enter the destination address in the **Query Builder** window (**addr.dst in 10.15.0.20**) or select the following

in each column and click **Add**: Connector = and, Attribute = Destination Address, Operator = in, and Value = 10.15.0.20. Click **Add** to add the query.

4. Click **Run Now** to run the report. The report will show all client hosts that have sent traffic to the sinkhole address, which indicates that they are most likely infected. You can now track down the hosts and check them for spyware.

5. To view scheduled reports that have run, select **Monitor** > **Reports**.

Custom Signatures

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

You can create custom threat signatures to detect and block specific traffic. When the firewall is managed by a Panorama management server, the ThreatID is mapped to the corresponding custom threat on the firewall to enable the firewall to generate a threat log populated with the configured custom ThreatID. Learn more by visiting our guide to Custom Application and Threat Signatures.

Monitor Advanced Threat Prevention

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Palo Alto Networks provides several options to monitor activity processed by Advanced Threat Prevention to accommodate intelligence retrieval for a range of products that rely on Advanced Threat Prevention and the associated data. Depending on the product platform, you can access high-level dashboards that also provide DNS request statistics and usage trends, including context into network activity, and DNS request details from specific users.

You can also view how Advanced Threat Prevention integrates with other Palo Alto Networks applications and security services to protect your organization from threats, as well as get a high-level view of the overall operational health of your deployment, through the Strata Cloud Manager Command Center. The command center functions as your NetSec homepage and provides a comprehensive summary of the health, security, and efficiency of your network, in an interactive visual dashboard with multiple data facets for easy, at-a-glace assessment.

For a high-level view of network activity, you can view the dashboard which provides visibility into the network's overall threat management data as well as various DNS trends. Each dashboard card provides a unique view into a threat's impact to your network, in a graphical report format. This provides an at-a-glace insight into the entities which are most affected by threats, based on application, user, as well as which security rules are enforcing your organization's policies.

Palo Alto Networks provides several methods to monitor the threat activity:

- The Strata Cloud Manager Command Center
- View Threat Logs
- View Advanced Threat Prevention Report
- Monitor Blocked IP Addresses
- Learn More About Threat Signatures
- Create Custom Reports Based on Threat Categories

View Threat Logs

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Threat categories classify different types of threat signatures to help you understand and draw connections between events threat signatures detect. Threat categories are subsets of the more broad threat signature types: spyware, vulnerability, and antivirus. Threat log entries display the **Threat Category** for each recorded event.

You can browse, search, and view Advanced Threat Prevention logs that are automatically generated when a threat is detected. Typically, this includes any qualifying threat signature match that a Threat Prevention feature, including Inline ML, analyzes unless it is specifically configured with a log severity level of none. Log entries provide numerous details about the event, including the threat level and, if applicable, the nature of threat.

- Strata Cloud Manager
- PAN-OS & Panorama

View Threat Logs (Cloud Management)

STEP 1 | Use the credentials associated with your Palo Alto Networks support account and log in to the Strata Cloud Manager on the hub.

> *For more information on using Activity dashboards, refer to the Log Viewer.*

STEP 2 | Filter threat logs based on the **Threat Category** or **Subtype** in Prisma Access.

1. Select **Incidents & Alerts** > **Log Viewer**.

2. Change the log type to be searched to **Threat**.

3. Create a search filter using one the threat signature subtypes used by the Antivirus, Anti-spyware, or Vulnerability Protection profiles (**antivirus**, **spyware**, and **vulnerability**, respectively) or based on the threat category using the query builder. For example, you can use `sub_type.value = 'spyware'` to view logs for threats that have been determined to be spyware. To search for other subtypes, replace spyware in the above example with another supported subtype (**vulnerability** or **spyware**). You can also search based on a specific **Threat Category**, such as an info-leak vulnerability by using the following query `threat_category.value = 'info-leak'`. For a list of valid

categories you can use, refer to Threat Signature Categories. Adjust the search criteria as necessary for your search, including additional query parameters (such as the severity level and action) along with a date range.

4. Run the query after you have finished assembling your filters.

5. Select a log entry from the results to view the log details.

6. The threat **Category** is displayed in the **Details** pane of the detailed log view. Other relevant details about the threat are displayed in their corresponding windows.

STEP 3 | Filter Threat logs by threat [categories] that have been detected using inline cloud analysis (spyware).

> *HTTP-based C2 traffic that was originally categorized with the threat name Inline Cloud Analyzed HTTP Command and Control Traffic Detection and is associated with multiple Threat IDs, is now separated into three unique threat names to correspond to the unique Threat IDs and more accurately describe the detections made by Advanced Threat Prevention: **Evasive HTTP C2 Traffic Detection** (Threat ID: 89950), **Evasive Cobalt Strike C2 Traffic Detection** (Threat ID: 89955, 89956, and 89957), and **Evasive Empire C2 Traffic Detection** (Threat ID: 89958).*
>
> *HTTP-based C2 traffic logs generated prior to December 11, 2023 will continue to be categorized with the threat name Inline Cloud Analyzed HTTP Command and Control Traffic Detection.*

1. Select **Incidents & Alerts** > **Log Viewer**.
2. Change the log type to be searched to **Threat**.
3. Create a search filter using a threat category used exclusively by Inline Cloud Analysis (spyware): `threat_category.value = 'inline-cloud-c2'`. You can further constrain the search by cross-referencing a Threat-ID value that corresponds to a specific C2 type. For example, `threat_category.value = 'inline-cloud-c2' AND Threat ID = 89958`, whereby 89958 indicates the Threat ID of evasive empire C2 traffic.
4. Select a log entry to view the details of a detected C2 threat.
5. The threat **Category** is displayed under the **General** pane of the log details. C2 threats that have been detected using inline cloud analysis have a threat category of inline-cloud-c2. You can cross-reference the Threat **ID** value in the **Details** pane to determine the specific type of C2 that has been detected.

STEP 4 | Filter Threat logs by threat [categories] that have been detected using inline cloud analysis (vulnerability).

1. Select **Incidents & Alerts** > **Log Viewer**.
2. Change the log type to be searched to **Threat**.
3. Create a search filter using a threat category used exclusively by Inline Cloud Analysis (vulnerability): `threat_category.value = 'inline-cloud-exploit'`.
4. Select a log entry to view the details of the detected command injection and SQL injection vulnerabilities. Inline exploit (SQL injection) threats have an ID of 99950 while inline exploit (command injection) threats have an ID of 99951.

View Threat Logs (NGFW (Managed by PAN-OS or Panorama))

◉ Filter Threat logs by threat category.

    1. Select **Monitor** > **Logs** > **Threat**.

    2. Add the Threat Category column so you can view the Threat Category for each log entry:

    3. To filter based on Threat Category:

        • Use the log query builder to add a filter with the **Attribute** Threat Category and in the **Value** field, enter a Threat Category.

        • Select the Threat Category of any log entry to add that category to the filter:

◉ Filter Threat logs by threat signature type.

    1. Select **Monitor** > **Logs** > **Threat**.

    2. Add the **Type** column, if it is not present, so you can view the threat signature category for each log entry:

    3. To filter based on the signature type:

        • Use the log query builder to add a filter with the **Attribute** of the threat signature category and in the **Value** field, enter a threat signature type. You can select from **vulnerability**, **virus**, and **spyware**, which corresponds to the signatures handled by your Vulnerability Protection, Antivirus, and Anti-Spyware security profiles.

        • Select the **Type** of any log entry to add that threat signature type to the filter. You can also manually build your query using the filter and threat signature type.

○ Filter Threat logs by threat [categories] that have been detected using inline cloud analysis (spyware).

📋 *HTTP-based C2 traffic that was originally categorized with the threat name Inline Cloud Analyzed HTTP Command and Control Traffic Detection and is associated with multiple Threat IDs, is now separated into three unique threat names to correspond to the unique Threat IDs and more accurately describe the detections made by Advanced Threat Prevention:* **Evasive HTTP C2 Traffic Detection** *(Threat ID: 89950),* **Evasive Cobalt Strike C2 Traffic Detection** *(Threat ID: 89955, 89956, and 89957), and* **Evasive Empire C2 Traffic Detection** *(Threat ID: 89958).*

If you do not install the update content or are reviewing HTTP-based C2 traffic logs generated prior to December 11, 2023 (the release date of the content update), all HTTP-based C2 traffic will continue to be categorized with the threat name Inline Cloud Analyzed HTTP Command and Control Traffic Detection.

1. Select **Monitor** > **Logs** > **Threat**. You can filter the logs based on certain characteristics of the threat. Consider the following examples:

   - Filter using (`category-of-threatid eq inline-cloud-c2`) to view logs for C2 threats that have been analyzed using the inline cloud analysis mechanism of Advanced Threat Prevention.

   - You can further constrain the search by cross-referencing a Threat-ID value that corresponds to a specific C2 type. For example, (`category-of-threatid eq inline-cloud-c2`) `and (name-of-threatid eq 89958)`, whereby 89958 indicates the Threat ID of evasive empire C2 traffic.

   - Filter using (`local_deep_learning eq yes`) to view logs for threats that have been analyzed using the Local Deep Analysis mechanism of Advanced Threat Prevention.

		RECEIVE TIME	THREAT CATEGORY	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY
		12/01 09:58:10	inline-cloud-c2	spyware	Inline Cloud Analyzed SSL Command and Control Traffic Detection	in-vwire	out-wire		443	ssl	alert	high
		12/01 09:57:00	inline-cloud-c2	spyware	Inline Cloud Analyzed HTTP Command and Control Traffic Detection	in-vwire	out-wire		80	web-browsing	alert	high

2. Select a log entry to view the details of a detected C2 threat.

3. The threat **Category** is displayed under the **Details** pane of the detailed log view. C2 threats that have been detected using inline cloud analysis have a threat category of

inline-cloud-c2. You can cross-reference the Threat **ID** value to determine the specific type of C2 that has been detected.

Details	
Threat Type	spyware
Threat ID/Name	Inline Cloud Analyzed HTTP Command and Control Traffic Detection
ID	89950 (View in Threat Vault)
Category	inline-cloud-c2
Content Version	AppThreat-8492-15511
Severity	high
Repeat Count	1
File Name	
URL	
Partial Hash	0
Pcap ID	0
Source UUID	
Destination UUID	
Dynamic User Group	
Network Slice ID SST	
Network Slice ID SD	
App Category	general-internet
App Subcategory	internet-utility
App Technology	browser-based
App Characteristic	used-by-malware,able-to-transfer-file,has-known-vulnerability,tunnel-other-application,pervasive-use
App Container	
App Risk	4
App SaaS	no
App Sanctioned State	no
Cloud Report ID	9411efa983ef1607abe84fd54f072f2d2ab16...

4. If the threat was analyzed using Local Deep Learning, the **Local Deep Learning Analyzed** field indicates yes.

General	
Session ID	164638
Action	alert
Host ID	
Application	web-browsing
Rule	rule1_vsys1
Rule UUID	0378c0bd-df0a-42f8-a1fb-11898d612714
Device SN	
IP Protocol	tcp
Log Action	
Generated Time	2024/01/30 15:32:49
Receive Time	2024/01/30 15:32:49
Tunnel Type	N/A
Cluster Name	
Local Deep Learning Analyzed	yes

- Monitor activity on the firewall for vulnerability exploits that have been detected using inline cloud analysis (vulnerability).
  1. Select **Monitor** > **Logs** > **Threat** and filter by (`category-of-threatid eq inline-cloud-exploit`) to view logs that have been analyzed using the inline cloud analysis mechanism of Advanced Threat Prevention. Inline exploit (SQL injection)

threats have an ID of 99950 while inline exploit (command injection) threats have an ID of 99951.

2. Select a log entry to view the details of a vulnerability exploit.

3. The threat **Category** is displayed under the **Details** pane of the detailed log view. Vulnerability exploits that have been detected using inline cloud analysis have a threat category of inline-cloud-exploit.

◉ Filter ACC activity by threat category.

1. Select **ACC** and add Threat Category as a global filter:

2. Select the Threat Category to filter all ACC tabs.

View Advanced Threat Prevention Report

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

The Advanced Threat Prevention Report is available though the Threat Vault API and provides detailed analysis and detection information, as well as information about the transaction, session, and other related processes. The report contain some or all of the information described in the following table based on the session information configured on the firewall that processed the file and the analysis details for the file in a JSON format.

> NGFWs do not have direct access to reports through PAN-OS; instead, you must reference the cloud_reportid associated with the threat log and use the Threat Vault API to search and retrieve the report.
>
> For Prisma Access (through the Strata Cloud Manager), the report is viewable from the log viewer (View Threat Logs). Log entries with a generated Advanced Threat Prevention report have a download link next to the report ID value under the **Cloud ReportID** column.

Report Heading	Description
General Information	Contains information about the firewall/security platform that processed the threat. • The cloud report ID number containing the Advanced Threat report data. • Error messages that might have been generated during creation of the report.
PAN-OS Information	Contains information about the firewall/security platform that processed the threat. • Firewall interface (IPv4/IPv6) • Content package version • Firewall Hostname • Firewall model • Serial Number

Report Heading	Description
	• PAN-OS version
Session Information	Contains session information based on the traffic as it traversed the firewall/security platform that forwarded the threat. The following options are available: • Source IP • Source Port • Destination IP • Destination Port • Session ID • Session Timestamp • Payload Type
Transaction Data	The transaction data provides an overview of the payload details and contains the detection service report(s). The following options are available: • Transaction ID • SHA256 hash of the payload
Detection Service Results	When threat analysis is performed by the Advanced Threat Prevention cloud, this section contains entries showing the analysis results. This includes the detection service report(s), which additionally provides the MITRE ATT&CK® classified techniques employed, as well as the payload details. Command and control detections for the Empire C2 framework show additional contextual information. This includes reports generated from both the staging and command (post exploitation) phase of an attack that occurs in separate sessions. The following information entries are available: • Attack Description—describes the nature of the C2 attack. • Attack Details—indicates the phase of the Empire C2 attack as well as describe the exchanges between the server and client. • Attack Evidences—lists behavior and actions consistent with known Empire C2.

Report Heading	Description
	Empire-based C2 is detected using a sub-module detector contained within the **Inline Cloud Analyzed HTTP Command and Control Traffic Detection** *analysis engine with a unique threat ID of 89958.*

Monitor Blocked IP Addresses

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

The firewall maintains a block list of source IP addresses that it's blocking. When the firewall blocks a source IP address, such as when you configure either of the following policy rules, the firewall blocks that traffic in hardware before those packets use CPU or packet buffer resources:

- A classified DoS Protection policy rule with the action to **Protect** (a classified DoS Protection policy specifies that incoming connections match a source IP address, destination IP address, or source and destination IP address pair, and is associated with a Classified DoS Protection profile, as described in DoS Protection Against Flooding of New Sessions).

- A Security Policy rule that uses a Vulnerability Protection profile

Hardware IP address blocking is supported on PA-3200 Series, PA-5200 Series, PA-5400 Series (excepting the PA-5450), and PA-7000 Series firewalls.

You can view the block list, get detailed information about an IP address on the block list, or view counts of addresses that hardware and software are blocking. You can delete an IP address from the list if you think it shouldn't be blocked. You can change the source of detailed information about addresses on the list. You can also change how long hardware blocks IP addresses.

◉ View block list entries.

1. Select **Monitor** > **Block IP List**.

   Entries on the block list indicate in the Type column whether they were blocked by hardware (hw) or software (sw).

2. View at the bottom of the screen:

   - Count of **Total Blocked IPs** out of the number of blocked IP addresses the firewall supports.

   - Percentage of the block list the firewall has used.

3. To filter the entries displayed, select a value in a column (which creates a filter in the **Filters** field) and Apply Filter (→). Otherwise, the firewall displays the first 1,000 entries.

4. Enter a **Page** number or click the arrows at the bottom of the screen to advance through pages of entries.

5. To view details about an address on the block list, hover over a Source IP address and click the down arrow link. Click the **Who Is** link, which displays Network Solutions Whois information about the address.

◉ Delete block list entries.

> *Delete an entry if you determine the IP address shouldn't be blocked. Then revise the policy rule that caused the firewall to block the address.*

1. Select **Monitor** > **Block IP List**.
2. Select one or more entries and click **Delete**.
3. (Optional) Select **Clear All** to remove all entries from the list.

◉ Disable or re-enable hardware IP address blocking for troubleshooting purposes.

> *While hardware IP address blocking is disabled, the firewall still performs any software IP address blocking you have configured.*

```
> set system setting hardware-acl-blocking [enable | disable]
```

> *To conserve CPU and packet buffer resources, leave hardware IP address blocking enabled unless Palo Alto Networks technical support asks you to disable it, for example, if they are debugging a traffic flow.*

○ Tune the number of seconds that IP addresses blocked by hardware remain on the block list (range is 1-3,600; default is 1).

```
> set system setting hardware-acl-blocking duration <seconds>
```

💡 *Maintain a shorter duration for hardware block list entries than software block list entries to reduce the likelihood of exceeding the blocking capacity of the hardware.*

○ Change the default website for finding more information about an IP address from Network Solutions Who Is to a different website.

```
# set deviceconfig system ip-address-lookup-url <url>
```

○ View counts of source IP addresses blocked by hardware and software, for example to see the rate of an attack.

View the total sum of IP address entries on the hardware block table and block list (blocked by hardware and software):

```
> show counter global name flow_dos_blk_num_entries
```

View the count of IP address entries on the hardware block table that were blocked by hardware:

```
> show counter global name flow_dos_blk_hw_entries
```

View the count of IP address entries on the block list that were blocked by software:

```
> show counter global name flow_dos_blk_sw_entries
```

○ View block list information per slot on a PA-7000 Series firewall.

```
> show dos-block-table software filter slot <slot-number>
```

Learn More About Threat Signatures

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

Firewall Threat logs record all threats the firewall detects based on threat signatures (Set Up Antivirus, Anti-Spyware, and Vulnerability Protection) and the ACC displays an overview of the top threats on your network. Each event the firewall records includes an ID that identifies the associated threat signature.

You can use the threat ID found with a Threat log or ACC entry to:

- Easily check if a threat signature is configured as an exception to your security policy (Create Threat Exceptions).

- Find the latest Threat Vault information about a specific threat. Because the Threat Vault is integrated with the firewall, you can view threat details directly in the firewall context or launch a Threat Vault search in a new browser window for a threat the firewall logged.

> *If a signature has been disabled, the signature UTID might be reused for a new signature.*
>
> *Review the content update release notes for notifications regarding new and disabled signatures. Signatures might disabled in cases where: the activity the signature detects has fallen out of use by attackers, the signature generated significant false positives, or the signature was consolidated with other like signatures into a single signature (signature optimization).*

STEP 1 | Confirm the firewall is connected to the Threat Vault.

Select **Device** > **Setup** > **Management** and edit the **Logging and Reporting** setting to **Enable Threat Vault Access**. Threat vault access is enabled by default.

STEP 2 | Find the threat ID for threats the firewall detects.

- To see each threat event the firewall detects based on threat signatures, select **Monitor** > **Logs** > **Threat**. You can find the ID for a threat entry listed in the ID column, or select the log entry to view log details, including the Threat ID.

- To see an overview of top threats on the network, select **ACC** > **Threat Activity** and take a look at the Threat Activity widget. The ID column displays the threat ID for each threat displayed.

- To see details for threats that you can configure as threat exceptions (meaning, the firewall enforces the threat differently than the default action defined for the threat signature), select **Objects** > **Security Profiles** > **Anti-Spyware/Vulnerability Protection**. **Add** or modify a profile and click the **Exceptions** tab to view configured exceptions. If no exceptions are configured, you can filter for threat signatures or select **Show all signatures**.

STEP 3 | Hover over a **Threat Name** or the threat **ID** to open the drop-down, and click **Exception** to review both the threat details and how the firewall is configured to enforce the threat.

For example, find out more about a top threat charted on the ACC:
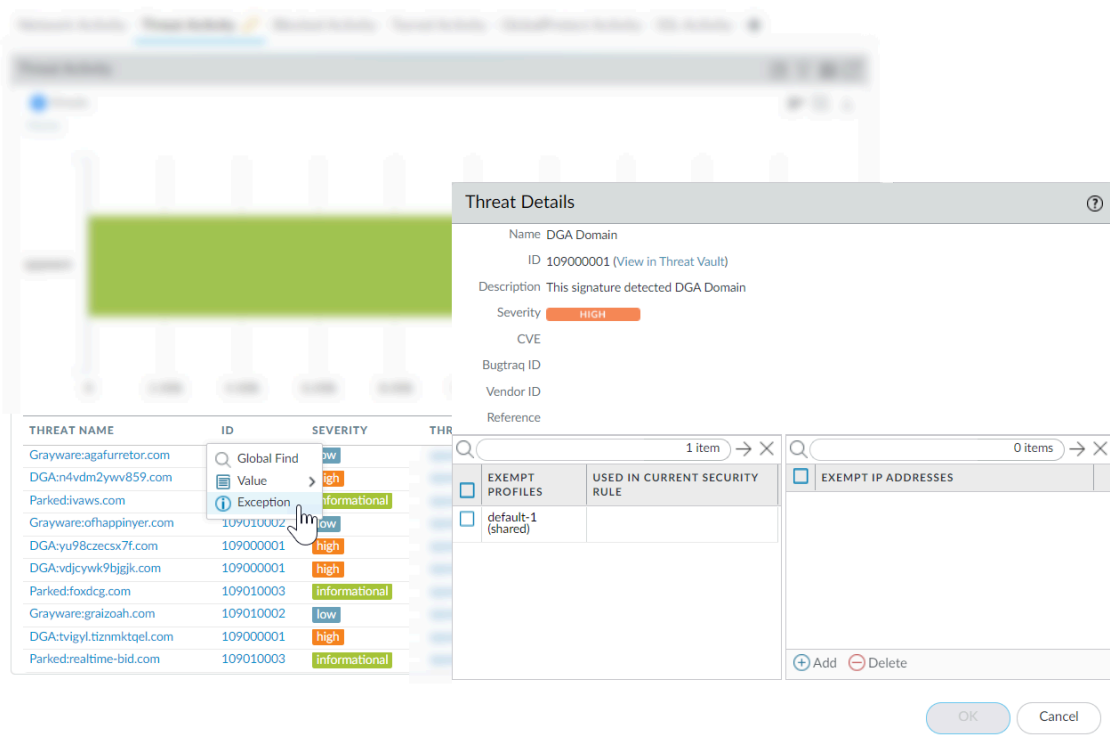
STEP 4 | Review the latest **Threat Details** for the threat and launch a Threat Vault search based on the threat ID.

- Threat details displayed include the latest Threat Vault information for the threat, resources you can use to learn more about the threat, and CVEs associated with the threat.

- Select **View in Threat Vault** to open a Threat Vault search in a new window and look up the latest information the Palo Alto Networks threat database has for this threat signature.

STEP 5 | Check if a threat signature is configured as an exception to your security policy.

- If the **Used in current security rule** column is clear, the firewall is enforcing the threat based on the recommended default signature action (for example, block or alert).

- A checkmark anywhere in the **Used in current security rule** column indicates that a security policy rule is configured to enforce a non-default action for the threat (for example, allow), based on the associated **Exempt Profiles** settings.

> *The **Used in security rule column** does not indicate if the Security policy rule is enabled, only if the Security policy rule is configured with the threat exception. Select **Policies > Security** to check if an indicated security policy rule is enabled.*

STEP 6 | **Add** an IP address on which to filter the threat exception or view existing **Exempt IP Addresses**.

Configure an exempt IP address to enforce a threat exception only when the associated session has either a matching source or destination IP address; for all other sessions, the threat is enforced based on the default signature action.

Create Custom Reports Based on Threat Categories

Where Can I Use This?	What Do I Need?
- NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	☐ Advanced Threat Prevention (for enhanced feature support) or Threat Prevention License

You can create custom reports on the firewall to generate (on demand) or to schedule (each night) reports based on attributes or key pieces of information that you want to retrieve and analyze.

◉ Create custom reports based on threat categories to receive information about specific types of threats that the firewall has detected.

1. Select **Monitor** > **Manage Custom** reports to add a new custom report or modify an existing one.

2. Choose the **Database** to use as the source for the custom report—in this case, select **Threat** from either of the two types of database sources, summary databases and Detailed logs. Summary database data is condensed to allow a faster response time when generating reports. Detailed logs take longer to generate but provide an itemized and complete set of data for each log entry.

3. In the Query Builder, add a report filter with the Attribute **Threat Category** and in the Value field, select a threat category on which to base your report.

4. To test the new report settings, click **Run Now**.

5. Click **OK** to save the report.